1 АНАЛІЗ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Призначення, структура, функції та умови функціонування корпоративної інформаційної системи

У найзагальнішому сенсі термін *корпорація* означає об'єднання підприємств, що працюють під централізованим управлінням та вирішують загальні завдання. Корпорація є складною, багатопрофільною структурою і внаслідок цього має розподілену ієрархічну систему управління [1].

Корпоративне управління визначається як система взаємовідносин між акціонерами, радою директорів і правлінням, визначені статутом, регламентом і офіційною політикою компанії, а також принципом верховенства права на основі прийнятої бізнес моделі.

Бізнес-модель – це опис підприємства, як складної системи, із заданою точністю. В рамках бізнес-моделі відображаються всі об'єкти (сутності), процеси, правила виконання операцій, існуюча стратегія розвитку, а також критерії оцінки ефективності функціонування системи. Форма представлення бізнес-моделі і рівень її деталізації визначаються цілями моделювання і прийнятою точкою зору.

Підприємства, відділення та адміністративні офіси, що входять в корпорацію, як правило, розташовані на достатньому видаленні один від одного. Їх інформаційний зв'язок один з одним утворює комунікаційну структуру корпорації, основою якої є *інформаційна система* [1].

Інформаційна модель – підмножина бізнес-моделі, що описує всі існуючі (в тому числі не формалізовані в документальному вигляді) інформаційні потоки на підприємстві, правила обробки і алгоритми маршрутизації всіх елементів інформаційного поля.

Інформаційна система (ІС) – це вся інфраструктура підприємства, задіяна в процесі управління всіма інформаційно-документальними потоками, що включає в

себе такі обов'язкові елементи [1]:

інформаційна модель, яка являє собою сукупність правил і алгоритмів функціонування ІС. Інформаційна модель включає в себе всі форми документів, структуру довідників і даних тощо;

регламент розвитку інформаційної моделі і правила внесення в неї змін;

кадрові ресурси (департамент розвитку, які залучаються консультанти), що відповідають за формування і розвиток інформаційної моделі;

програмне забезпечення, конфігурація якого відповідає вимогам інформаційної моделі (програмне забезпечення є основним рушієм і, одночасно, механізмом управління ІС). Крім того, завжди існують вимоги до постачальника програмного забезпечення, які регламентують процедуру технічної і призначеної для користувача підтримки впродовж усього життєвого циклу;

кадрові ресурси, що відповідають за налаштування і адаптацію програмного забезпечення, і його відповідність затвердженій інформаційній моделі;

регламент внесення змін до структури (специфічні настройки, структури баз даних і т.д.) і конфігурацію програмного забезпечення та склад його функціональних модулів;

апаратна база, яка відповідає вимогам по експлуатації програмного забезпечення (комп'ютери на робочих місцях, периферія, канали телекомунікацій, системне програмне забезпечення та СУБД);

кадрові ресурси, включаючи персонал по обслуговуванню апаратної бази;

правила використання програмного забезпечення і призначені для користувача інструкції, регламент навчання і сертифікації користувачів.

Ресурси корпорацій включають: матеріальні (матеріали, готова продукція, основні засоби); фінансові; людські (персонал); знання (ноу-хау); корпоративна інформаційна система.

Система управління будь-якої компанії включає три основні підсистеми [1]:

планування продажів і операцій. Це загальний план функціонування підприємства, що встановлює обсяги виготовлення готової продукції. Головним тут є планування попиту і оцінка ресурсів, необхідних для задоволення попиту. Тут

же створюється основний виробничий план, який визначає, які вироби, в якій кількості і в які терміни потрібно зробити;

детальне планування необхідних ресурсів (матеріалів, виробничих потужностей, трудових ресурсів тощо). Складений план визначає час і обсяг замовлень для всіх матеріалів і комплектуючих, необхідних для реалізації основного виробничого плану;

управління виконанням планів в процесі виробництва і закупівель (постачання).

Всі ці робочі процеси вищеперелічених підсистем реалізуються на основі корпоративної інформаційної системи.

Корпоративні інформаційні системи (КІС) – це інтегровані системи управління територіально розподіленої корпорацією, засновані на поглибленому аналізі даних, широке використання систем інформаційної підтримки прийняття рішень, електронних документообігу та діловодстві. КІС покликані об'єднати стратегію управління підприємством і передові інформаційні технології [1].

Корпоративна інформаційна система – це сукупність технічних і програмних засобів підприємства, що реалізують ідеї і методи автоматизації.

Комплексна автоматизація бізнес процесів підприємства на базі сучасної апаратної та програмної підтримки може називатися по-різному. В даний час поряд з назвою корпоративні інформаційні системи вживаються, наприклад, такі назви [1]:

автоматизовані системи управління (АСУ);

інтегровані системи управління (ІСУ);

інтегровані інформаційні системи (ІІС);

інформаційні системи управління підприємством (ІСУП).

Головне завдання КІС – ефективне управління всіма ресурсами підприємства (матеріально-технічними, фінансовими, технологічними і інтелектуальними) для отримання максимального прибутку і задоволення матеріальних і професійних потреб усіх співробітників підприємства.

КІС за своїм складом є сукупністю різних програмно-апаратних платформ,

універсальних і спеціалізованих додатків різних розробників, інтегрованих в єдину інформаційно систему, яка найкращим чином вирішує в деякому роді унікальну задачу кожного конкретного підприємства. Тобто, КІС – людино-машинна система і інструмент підтримки інтелектуальної діяльності людини, яка під його впливом повинна [1]:

накопичувати певний досвід і формалізовані знання;

постійно вдосконалюватися і розвиватися;

швидко адаптуватися до мінливих умов зовнішнього середовища і нових потреб підприємства.

Комплексна автоматизація підприємства має на увазі переклад в площину комп'ютерних технологій всіх основних ділових процесів організації. І використання спеціальних програмних засобів, що забезпечують інформаційну підтримку бізнес-процесів, як основи КІС представляється найбільш виправданим і ефективним. Сучасні системи управління бізнес-процесами дозволяють інтегрувати навколо себе різне програмне забезпечення, формуючи єдину інформаційну систему. Тим самим вирішуються проблеми координації діяльності співробітників і підрозділів, забезпечення їх необхідною інформацією і контролю виконавської дисципліни, а керівництво отримує своєчасний доступ до достовірними даними про хід виробничого процесу і має кошти для оперативного прийняття і втілення в життя своїх рішень [1].

Автоматизований комплекс засобів має являти собою гнучку відкриту структуру, яку можна перебудовувати і доповнювати новими модулями або зовнішнім програмним забезпеченням.

Під *корпоративною інформаційною системою* розуміють інформаційну систему організації, що відповідає наступним мінімальним переліком вимог [1]:

функціональна повнота системи;

надійна система захисту інформації;

наявність інструментальних засобів адаптації та супроводу системи;

реалізація віддаленого доступу і роботи в розподілених мережах;

забезпечення обміну даними між розробленими інформаційними системами,

програмними продуктами, що функціонують в організації тощо;

можливість консолідації інформації;

наявність спеціальних засобів аналізу стану системи в процесі експлуатації.

Функціональна повнота системи забезпечується [1]:

виконанням міжнародних стандартів управлінського обліку MRP II, ERP, CSRP;

автоматизацією в рамках системи вирішення завдань планування, бюджетування, прогнозування, оперативного (управлінського) обліку, бухгалтерського обліку, статистичного обліку та фінансового-економічного аналізу;

формуванням і веденням обліку за вітчизняними та міжнародними стандартами тощо.

Найбільш розвинені корпоративні інформаційні системи призначені для автоматизації всіх функцій управління організацією: від науково-технічної та маркетингової підготовки її діяльності до реалізації її продукції і послуг. В даний час КІС мають в основному економічну і виробничу спрямованість.

Розглядаючи архітектуру великих організацій, прийнято використовувати поняття «корпоративна архітектура». Її можна представити у вигляді сукупності декількох типів архітектур [2]:

бізнес архітектура (Business architecture);

IT-архітектура (Information Technology architecture);

архітектура даних (Data architecture);

програмна архітектура (Software architecture);

технічна архітектура (Hardware architecture).

Модель корпоративної архітектури представлена на рис. 1.1.

Технічна архітектура є першим рівнем архітектури інформаційної системи. Вона описує всі апаратні засоби, що використовуються при виконанні заявленого набору функцій, а також включає засобу забезпечення мережної взаємодії й надійності. У технічній архітектурі вказуються периферійні пристрої, мережні комутатори й маршрутизатори, жорсткі диски, оперативна пам’ять, процесори,

сполучні кабелі, джерела безперебійного живлення тощо.

Рис. 1.1. Модель корпоративної інформаційної системи [2]

Програмна архітектура являє собою сукупність комп'ютерних програм, призначених для рішення конкретних завдань. Даний тип архітектури призначений для опису додатків, що входять до складу інформаційної системи. На даному рівні описують програмні інтерфейси, компоненти й поведінку.

Архітектура даних поєднує в собі як фізичні сховища даних, так і засоби керування даними. Крім того, до неї входять логічні сховища даних, а при орієнтованості розглянутої компанії на роботу зі знаннями, може бути виділений окремий рівень – архітектура знань (Knowledge architecture). На цьому рівні описуються логічні й фізичні моделі даних, визначаються правила цілісності, складаються обмеження для даних.

Слід особливо виділити рівень *IT-архітектури*, оскільки він є сполучним.

На ньому формується базовий набір сервісів, які використовуються як на рівні програмної архітектури, так і на рівні архітектури даних. Якщо будь-яка особливість функціонування для цих двох рівнів не була передбачена, то сильно зростає ймовірність збоїв у роботі, а, отже, втрат для бізнесу. У деяких випадках неможливо розділити IT-архітектуру й архітектуру окремого додатка. Таке можливо при високому ступені інтеграції додатків. Прикладом IT-архітектури

може служити SharePoint від Microsoft. Цей продукт надає сервіси для спільної роботи й зберігання інформації, що є дуже важливим аспектом функціонування будь-якої компанії. Його базові системні модулі відносяться до IT-архітектури, а користувальницькі – до програмного.

Основною функцією IT-архітектури є забезпечення функціонування важливих бізнесів-додатків для досягнення позначених бізнесів-цілей. Якщо деяка функція потрібна відразу в декількох додатках, то її доцільно перенести на рівень IT-архітектури, тим самим підвищивши інтеграцію системи й знизити складність архітектури додатків.

Останнім в ієрархії є *рівень бізнес-архітектури* або *архітектури бізнесів-процесів*. На цьому рівні визначаються стратегії ведення бізнесу, способи керування, принципи організації й ключові процеси, що представляють для бізнесу величезну важливість.

Технологія – комплекс наукових та інженерних знань, втілених в способах і засобах праці, наборах матеріально-речових факторів виробництва, видах їх поєднання для створення певного продукту або послуги [3].

До сучасної технології висуваються наступні вимоги [3]:

високий ступінь поділу процесу на стадії (фази);

системна повнота (цілісність) процесу, який повинен включати весь набір елементів, що забезпечують необхідну завершеність дій людини в досягненні поставленої мети;

регулярність процесу і однозначність його фаз, що дозволяють застосовувати середні величини при охарактеризуванні цих фаз, а отже їх стандартизації і уніфікації;

технологія є нерозривно пов'язаною із процесом – сукупністю дій, які виконуються в часі;

технологічний процес здійснюється в штучних системах, створених для забезпечення реалізації певних потреб.

Зазначені вище властивості визначають характеристики технологічних процесів [3]:

поділ процесу на внутрішні взаємозв'язані стани, фази, операції, що забезпечують оптимальну або близьку до оптимальної динаміку розвитку процесу, а також визначають раціональні межі вимог до персоналу, що працюватиме з даною технологією;

координування і поетапне виконання дій та операцій, спрямованих на досягнення необхідного результату, причому послідовність дій базується на логіці функціонування і розвитку визначеного процесу;

однозначність виконання наявних в технології процедур і операцій, що є неодмінною і вирішальною умовою досягнення результатів у відповідності з визначеними для цього нормами і нормативами.

Так можна інтерпретувати поняття технології в широкому сенсі. З іншого боку, в більш вузькому сенсі означення технології формулюється наступним чином [3]:

Технологія – це набір способів, засобів вибору і здійснення керуючого процесу з множини можливих його реалізацій.

В основі будь-якого процесу лежить визначена технологія, до компонентів якої відносяться [3]:

мета реалізації процесу;

предмет, що підлягає технологічним змінам;

способи і методи впливу;

засоби технологічного впливу;

впорядкованість і організація, які протиставлені стихійним процесам.

1.2. Аналіз загроз процесам функціонування корпоративних інформаційних системах

За метою впливу розрізняють три основні типи загроз безпеці інформаційних систем [4]: загрози порушення конфіденційності інформації; загрози порушення цілісності інформації; загрози порушення працездатності системи (відмови в обслуговуванні).

Загрози порушення конфіденційності направлені на розголошення конфіденційної чи секретної інформації. При реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступ. В термінах комп'ютерної безпеки загроза порушення конфіденційності проявляється щоразу, коли отримано несанкціонований доступ до деякої закритої інформації, що зберігається в комп'ютерній системі чи передається від однієї комп'ютерної системи до іншої.

Загрози порушення цілісності інформації, що зберігається в комп'ютерній системі чи передається по каналу зв'язку, направлені на її зміну чи спотворення, що приводить до порушення її якості чи повного знищення. Цілісність інформації може бути порушена спеціально зловмисноком, а також в результаті впливу зовнішнього середовища, що оточує систему. Ця загроза є особливо актуальна для систем передачі інформації – комп'ютерних мереж та систем телекомунікацій. Зумисні порушення цілісності інформації не слід плутати з її санкціонованою зміною, яка здійснюється повноважними особами з обґрунтованою метою.

Загрози порушення працездатності (відмова в обслуговуванні) направлені на створення таких ситуацій, коли певні навмисні дії або знижують працездатність ІС, або блокують доступ до її ресурсів. Наприклад, якщо один користувач системи робить спробу отримати доступ до деякої служби, а інший здійснює дії з блокування цього доступу, то перший користувач отримує відмову в обслуговуванні. Блокування доступу до ресурса може бути постійним чи тимчасовим.

Порушення конфіденційності та цілісності інформації, а також доступності і цілісності певних ресурсів ІС можуть бути викликані різними небезпечними впливами на інформаційну систему. Сучасні автоматизовані системи обробки інформації представляють собою складну систему, що складається з великої кількості компонент різного ступеня автономності, які зв'язані між собою та обмінюються даними. Практично кожний компонент може піддаватися зовнішньому впливу чи вийти з ладу. Компоненти інформаційної системи можна розділити на такі групи: апаратні засоби; програмне забезпечення; дані; персонал.

Небезпечні впливи на ІС можна поділити на випадкові та зловмисні. Аналіз досвіду проектування, виготовлення та експлуатації інформаційних систем показує, що інформація піддається різним випадковим впливам на всіх етапах функціонування інформаційної системи. Причинами випадкових впливів можуть бути: аварійні ситуації, пов'язані зі стихійними лихами та відключеннями електричного живлення; відмови та збої апаратури; помилки в програмному забезпеченні; помилки в роботі обслуговуючого персоналу та користувачів; завади в лініях зв'язку, спричинені впливом зовнішнього середовища.

Навмисні загрози пов'язані з цілеспрямованими діями порушника. Порушником може бути співробітник, відвідувач, конкурент, найманець тощо. Дії порушника можуть бути зумовлені різними мотивами: невдоволенням співробітника своєю кар'єрою, матеріальною зацікавленістю, цікавістю, конкурентною боротьбою, прагненням самоствердження та ін. Виходячи з можливості виникнення найнебезпечнішої ситуації, зумовленої діями порушника, можна скласти гіпотетичну модель потенційного порушника: кваліфікація порушника може бути на рівні розробника даної системи; порушником може бути як стороння особа, так і законний користувач системи; порушнику відома інформація про принципи роботи системи; порушник вибирає найслабшу ланку в захисті.

Можна виділити такі приклади навмисних загроз [5]: несанкціонований доступ сторонніх осіб, що не належать до числа співробітників, та ознайомлення з конфіденційною інформацією; ознайомлення співробітників з інформацією, до якої вони не повинні мати доступ; несанкціоноване копіювання програм і даних; викрадення носіїв інформації, що містять конфіденційну інформацію; викрадення роздрукованих документів; навмисне знищення інформації; несанкціонована модифікація співробітниками фінансових документів, звітності та баз даних; фальсифікація повідомлень, що передаються по каналах зв'язку; відмова від авторства повідомлення, переданого каналом зв'язку; відмова від факту отримання інформації; пошкодження інформації, викликане впливом вірусів; пошкодження архівної інформації, розміщеної на змінних носіях; викрадення обладнання.

Несанкціонований доступ є найбільш розповсюдженим та різностороннім видом комп'ютерних порушень. Суть несанкціонованого доступу полягає в отриманні користувачем (порушником) доступу до об'єкту з порушенням правил розмежування доступу, встановлених у відповідності до прийнятої в організації політики безпеки [Error: Reference source not found]. Несанкціонований доступ використовує будь-яку помилку в системі захисту та можливий при нераціональному виборі засобів захисту, некоректному їх встановленні та настроюванні. Несанкціонований доступ може бути здійснений як штатними засобами ІС, так і спеціально створеними апаратними і програмними засобами.

Наведемо перелік основних каналів несанкціонованого доступу, через які зловмисник може отримати доступ до компонентів ІС та здійснити крадіжку, модифікацію і/або пошкодження інформації: усі штатні канали доступу до інформації (комп'ютери користувачів, оператора, адміністратора системи; засоби відображення та документування інформації; канали зв'язку) при їх використанні порушниками, а також законними користувачами за межами їх повноважень; технологічні пульти управління; лінії зв'язку між апаратними засобами ІС; побічні електромагнітні випромінювання від апаратури, ліній зв'язку, мереж електричного живлення, заземлення тощо.

Із всих способів та прийомів несанкціонованого доступу зупинимося на найбільш розповсюджених та зв'язаних між собою порушеннях: перехоплення паролів; «маскарад»; незаконне використання привілеїв.

Перехоплення паролів здійснюється спеціально розробленими програмами. При спробі законного користувача ввійти в систему програма-перехоплювач імітує на екрані введення логіну та паролю користувача, які пересилаються власнику програми-перехоплювача після чого на екран виводиться повідомлення про помилку і управління повертається операційній системі. Користувач вважає, що допустив помилку при введенні паролю. Він повторює введення і отримує доступ в систему. Власник програми-перехоплювача, отримавши логін та пароль законного власника, може тепер їх використовувати в своїх цілях. Існують й інші способи перехоплення паролів.

«***Маскарад»*** – це виконання якихось дій одним користувачем від імені іншого, що має відповідні повноваження. Метою «маскараду» є приписування якихось дій іншому користувачу або присвоєння повноважень та привілеїв іншого користувача. Прикладами реалізації «маскараду» є: вхід в систему під іменем та паролем іншого користувача (такому «маскараду» передує перехоплення паролю); передача повідомлень в мережі від імені іншого користувача.

«Маскарад» є особливо небезпечним в банківських системах електронних платежів, де неправильна ідентифікація клієнта із-за «маскараду» зловмисника може привести до великих втрат законного клієнта банку.

Незаконне використання привілеїв. Більшість систем захисту встановлюють певні набори привілеїв для виконання заданих функцій. Кожний користувач отримує свій набір привілеїв: звичайні користувачі – мінімальний, адміністратори – максимальний. Несанкціоноване захоплення привілеїв, наприклад засобами «маскараду», приводить до можливості виконання порушником певних дій в обхід системи захисту. Слід зазначити, що незаконне захоплення привілеїв можливе або за наявності помилок в системі захисту, або із-за халатності адміністратора при управлінні системою та призначенні привілеїв.

Окремо слід зупинитися на загрозах, яким можуть піддаватися комп’ютерні мережі. Основна особливість будь-якої комп’ютерної мережі полягає в тому, що її компоненти розподілені в просторі. При вторгненні в комп’ютерну мережу зловмисник може використовувати як пасивні, так і активні методи вторгнення. При ***пасивному вторгненні*** (перехопленні інформації) порушник тільки спостерігає за проходженням інформації по каналу зв’язку, не втручаючись ні в інформаційний потік, ні в зміст інформації. Як правило, зловмисник може визначити пункти призначення та ідентифікатори або тільки факт проходження повідомлення, його довжину та частоту обміну, якщо зміст повідомлення розпізнати неможливо, – виконати аналіз трафіку (потоку повідомлень) в даному каналі.

При ***активному вторгненні*** порушник прагне підмінити інформацію, що передається в повідомленні. Він може вибірково модифікувати чи змінювати

повідомлення, затримувати чи змінювати порядок слідування повідомлень. Зловмисник може також анулювати і затримувати усі повідомлення, що передаються по каналу. Такі дії можна кваліфікувати як відмову в передачі повідомлень.

Комп'ютерні мережі характерні тим, що крім звичайних локальних атак, які здійснюються в межах однієї системи, проти об'єктів мереж здійснюють так звані, ***віддалені атаки***. Зловмисник може перебувати за тисячі кілометрів від атакованого об'єкта, при цьому нападу може піддаватися не тільки конкретний комп'ютер, а й інформація, що передаються по мережним каналам зв'язку. Під віддаленою атакою розуміють інформаційний зловмисний вплив на розподілену комп'ютерну мережу, який здійснюється програмно з використанням каналів зв'язку.

У табл. 1.2 показані основні шляхи реалізації загроз безпеці ІС при впливі на її компоненти. Ця таблиця дає тільки загальну картину того, що може відбутися з системою, а конкретні обставини та особливості повинні розглядатися окремо.

Таблиця 1.2.

Шляхи реалізації загроз безпеці ІС

Об'єкти впливу	Порушення конфіденційності інформації	Порушення цілісності інформації	Порушення працездатності системи
Апаратні засоби	Несанкціонований доступ – підключення; використання ресурсів; викрадення носіїв	Несанкціонований доступ – підключення; використання ресурсів; модифікація, зміна режимів	Несанкціонований доступ – зміна режимів; виведення з ладу; пошкодження
Програмне забезпечення	Несанкціонований доступ –	Несанкціонований доступ – впровадження	Несанкціонований доступ –

	копіювання; викрадення; перехоплення	„троянських коней“, „вірусів“, „черв’яків“	спотворення; знищення; підміна
Дані	Несанкціонований доступ – копіювання; викрадення; перехоплення	Несанкціонований доступ – спотворення; модифікація	Несанкціонований доступ – спотворення; знищення; підміна
Персонал	Розголошення; передача відомостей про захист; халатність	«Маскарад»; вербування; підкуп персоналу	Покидання робочого місця; фізичне усунення

У табл. 1.2 наведено специфічні назви та терміни: «троянський кінь», «вірус», «черв’як». Хоча ці назви мають жаргонний відтінок, вони уже ввійшли в загальноприйнятий комп’ютерний лексикон. Дамо коротку характеристику цих розповсюджених загроз безпеці ІС.

«***Троянський кінь»*** представляє собою програму, яка поряд з діями, описаними в її документації, виконує деякі інші дії, що ведуть до порушення безпеки системи та деструктивних результатів. Аналогія такої програми з давньогрецьким «троянським конем» повністю виправдана, оскільки в обидвох випадках оболонка, що не викликає підозр, містить в собі серйозну загрозу. Термін «троянський кінь» було вперше використано Даном Едвардсом, який пізніше став співробітником Агенства Національної Безпеки США. «Троянський кінь» використовує обман для того, щоб змустити користувача запустити програму з прихованою загрозою всередині. Зазвичай для цього стверджується, що така програма виконує деякі корисні функції. Зокрема, такі програми маскуються під якісь корисні утиліти.

Небезпека «троянського коня» полягає в додатковому блоці команд, вбудованому у вихідну корисну програму, яка потім надається користувачам. Цей блок команд може спрацьовувати при настанні якоїсь умови (дати, стану системи) або по команді ззовні. Користувач, який запустив таку програму, піддає небезпеці як свої ресурси, так і всю ІС в цілому. Наведемо для прикладу деякі деструктивні функції, що реалізуються «троянськими конями» [6]: ***знищення інформації***. Вибір об'єктів та способів знищення визначається фантазією та цілями автора зловмисної програми; ***перехоплення та передача інформації***. Зокрема, відомі програми, які здійснюють перехоплення паролів, що набираються на клавіатурі; ***цілеспрямована модифікація тексту програми***, яка реалізує функції безпеки та захисту системи.

Загалом, «троянські коні» завдають збитки ІС шляхом викрадення інформації та явного пошкодження програмного забезпечення системи. «Троянський кінь» є однією з найнебезпечніших загроз безпеці ІС. Радикальний спосіб захисту від цієї загрози полягає у створенні замкнутого середовища виконання програм, які повинні зберігатися і захищатися від несанкціонованого доступу. При цьому встановлення нового програмного забезпечення на комп'ютер повинно бути дозволено тільки адміністраторам, чого зазвичай складно досягти.

Комп'ютерні «віруси» – це певний тип програмних об'єктів, які володіють рядом властивостей, притаманних живим організмам, – вони народжуються, розмножуються та помирають. Термін «вірус» стосовно до комп'ютерів був запропонований Фредом Коеном із Університету Південної Каліфорнії. Історично перше визначення, дане Ф. Коеном звучало так: «Комп'ютерний вірус – це програма, яка може заражати інші програми, змінюючи їх шляхом включення в них своєї, можливо, зміненої копії, причому остання зберігає здатність до подальшого розмноження» [7]. Ключовими поняттями у визначенні комп'ютерного вірусу є здатність вірусу до саморозмноження та модифікації коду заражених програм.

Мережний «черв'як» представляє собою різновид програми-вірусу, яка розповсюджується глобальною мережею і не залишає своєї копії на магнітному носії (хоча є й інші варіанти «черв'яків», які зберігаються на фізичних носіях у вигляді файлів). Перші варіанти «черв'яків» були розроблені для пошуку в мережі

інших комп'ютерів з вільними ресурсами щоб забезпечувати можливість проведення розподілених обчислень. При правильному використанні технологія «черв'яків» може бути надзвичайно корисною. Наприклад, «черв'як» World Wide Web Worm формує індекс пошуку ділянок Web. Проте «черв'як» легко перетворюється у шкідливу програму.

Мережні «черв'яки» є найнебезпечнішим видом зловмисних програм, оскільки об'єктом їх нападу може стати будь-який з величезної кількості комп'ютерів, підключених до глобальної мережі Інтернет, чи інших мереж. Для захисту від «черв'яка» застосовують засоби, направлені на блокування несанкціонованого доступу до внутрішньої мережі.

Слід зазначити, що «троянські коні», комп'ютерні віруси та мережні «черв'яки» відносяться до найнебезпечніших загроз ІС. Для захисту від зловмисних програм необхідно застосовувати ряд заходів: виключення несанкціонованого доступу до виконуваних файлів; тестування нових програм; контроль цілісності виконуваних файлів та системних областей; створення замкнутого середовища виконання програм [8].

1.3. Аналіз проблеми розслідування на кіберінциденти в корпоративній інформаційній системі

Згідно зі звітом IBM за 2019 рік, в середньому через дії хакерів підприємства зазнають збитків у розмірі 239 мільйонів доларів. Однак фінансові втрати - не єдине, про що варто турбуватися. Компаніям потрібно близько 512 годин (приблизно 22 дня), щоб відновити працездатність своїх систем, що тягне за собою неможливість вести справи в штатному режимі і чималих збитків репутації.

Так, наприклад, норвезька компанія Norsk Hydro, що займається виробництвом алюмінію, в березні 2019 року піддалася атаці зловмисників, які використовували шифрувальник LockerGoga. Результатом стали фінансових

збитків майже в 66 мільйонів доларів, а також зупинене виробництво на частини фабрик і тимчасовий перехід в ручний режим роботи.

Крім вірусів-шифрувальників небезпеку становлять троянські та шпигунські програми, перехоплювачі і багато іншого.

Атаки організованих угруповань звуться APT (Advanced Persistent Threat), що в перекладі означає «цільова кібератака». Такі інциденти - серйозна проблема в сфері інформаційної безпеки, яка турбує не тільки великі корпорації: під прицілом хакерів знаходяться також підприємства середнього і малого бізнесу.

Організовані угрупування вибирають метою кібератак компанії в різноманітних сферах, таких як охорона здоров'я, IT, освіту та інші. Однією з основних і найбільш часто зустрічаються завдань злочинців є крадіжка конфіденційних відомостей і подальша їх продаж. Як же хакери потрапляють в корпоративну мережу і, тим більше, як в їх руках опиняються важливі дані?

Фізичні носії втратили свою актуальність, тому на сучасному етапі можна виділити три основні канали проникнення шкідливих програм в мережу. Перший - підбір пароля до віртуальної приватної мережі (VPN) і / або віддаленого робочого столу (RDP), другий - перехід користувача по зараженим посиланнях в будь-яких браузерах, третій, найбільш поширений, - розсилка фішингових листів.

Виходячи з того що найпопулярнішим вектором зараження є фішингові листи, типова атака в більшості випадків виглядає наступним чином: співробітник отримує на електронну пошту лист з вкладенням, яке має цілком очікуване для нього ім'я: «Копії документів», «Зарплатна відомість», «Товарна накладна »і ін. Адреса електронної пошти не викликає підозр, бо був попередньо підроблений так, що при побіжному погляді здасться співробітнику знайомим. Однак всередині листи - зовсім не документи, а ретельно замаскований шкідливий код, виконання якого призводить до початку зараження системи. Коли вірус закріплюється в комп'ютері жертви, він з'єднується зі своїм керівником сервером і повідомляє зловмисника про успішне проникнення в систему, після чого той, використовуючи реалізовані у шкідливій програмі функції, здійснює задумане.

Які дії необхідно зробити, якщо помічена підозріла активність в корпоративній мережі? В першу чергу слід негайно приступити до збору інформації про інцидент. В ході дослідження необхідно виявити канал впровадження шкідливої програми в мережу (початковий вектор атаки), ідентифікувати тип програмного забезпечення, задіяного зловмисниками, зрозуміти, які системи постраждали, визначити стадію атаки і розмір отриманого збитку.

Само по собі реагування на кібератаку можна розділити на кілька кроків:

- виявлення підозрілої активності на комп'ютері;
- імовірно спричиненої діяльністю шкідливої програми;
- ізоляція зараженої машини від корпоративної мережі;
- збір первинної інформації про вірус;
- видалення шкідливого об'єкта; -приведення систем в первісний стан;
- аналіз підсумків інциденту.

Збір інформації є найбільш важливим етапом розслідування, так як від отриманих в ході цього етапу даних залежить вся подальша робота відділу безпеки. Розглянемо докладніше, якими інструментами можна скористатися для дослідження персональних комп'ютерів.

Почнемо ми, мабуть, з програмного забезпечення для початкового реагування, яке допоможе нам виявити сліди, що вказують на роботу шкідливих програм.

Одним із зручних інструментів для дослідження комп'ютера під керуванням ОС Windows є AVZ - антивірусна утиліта, що дозволяє зібрати дані з таких модулів, як диспетчер процесів, менеджери автозапуску, планувальника завдань, впроваджених динамічних бібліотек, так само як і багатьох інших.

Корисним в дослідженні буде набір програм Sysinternals Suite, що включає в себе кілька безкоштовних програмних засобів, які можуть бути використані при зборі первинної інформації про інцидент. PSLoglist, наприклад, дозволяє переглянути вміст системного журналу Windows. Process Monitor - інструмент для спостереження за різними процесами в реальному часі, а Process Explorer, в свою

чергу, є утилітою не тільки для аналізу активності процесів в середовищі операційної системи Windows, але і для управління ними. Autoruns відображає все, що здатне автоматично запускатися на комп'ютері при його включенні: програми, модулі, різні системні служби і призначені завдання в ОС Windows. Таким чином, набір Sysinternals Suite допомагає провести багатостороннє дослідження і зібрати велику кількість первинної інформації.

Також варто відзначити програму GMER, яка дозволяє переглянути список запущених процесів, завантажених ними програмних модулів і створених потоків виконання, а також провести огляд файлової системи, списку сервісів, автоматично запускаються програм і реєстру ОС.

Коли сліди шкідливої програми виявлені, необхідно підготувати матеріал для подальшого дослідження. У цьому нам допоможуть утиліти для зняття образів жорстких дисків і дампов пам'яті.

До таких програм відноситься GRR Rapid Response, призначена для віддаленого аналізу оперативної пам'яті комп'ютера, системного реєстру і жорсткого диска за допомогою вбудованих утиліт Rekall і The Sleuth Kit.

Одним з найбільш поширених інструментів для зняття образу жорсткого диска в середовищі ОС Windows є FTK Imager, що входить в пакет Forensic Toolkit.

Для комп'ютерів, які базуються на Linux, також існують програмні засоби для вирішення зазначених завдань - dc3dd і ddrescue. За допомогою даних утиліт можна скопіювати розділи жорсткого диска ПК, в тому числі і приховані.

Щоб дослідити дані із знятих образів дисків, необхідно мати в арсеналі ще ряд програм, за допомогою яких можна провести їх розбір (парсинг) і зберегти результати для подальшої обробки.

Розглянемо ПО, яке ми побіжно згадували, коли говорили про GRR Rapid Response, - The Sleuth Kit (TSK). Воно дозволяє провести аналіз не тільки образів дисків, але і даних файлової системи.

Однією із зручних оболонок для TSK серед фахівців вважається Autopsy, яка забезпечує візуальне оформлення результатів роботи пакета The Sleuth Kit.

Додаток дозволяє аналізувати образи дисків і проводити дослідження накопичувача на «живий» системі.

Ще одним інструментом для вивчення даних на персональних комп'ютерах є Reg Ripper. Він працює з файлами реєстру Windows і витягує інформацію з його гілок.

Проте витяг повного образу персонального комп'ютера займає величезну кількість часу. У ситуації розгортається кібератаки зволікання неприпустимо, а зняття образу диска і його повний парсинг за допомогою, наприклад, Autopsy може тривати аж до декількох діб. Більш того, результати збору інформації при цьому вкрай слабо інтерпретуються, що тільки ускладнює завдання їх обробки і, отже, швидкого завершення розслідування. Відповідно, така втрата дорогоцінного часу може перешкодити своєчасному реагуванню на інцидент і привести до того, що атака кіберзлочинців увінчається успіхом, а компанія, в свою чергу, понесе величезні збитки.

Сучасний робочий процес проходить в основному в цифровому просторі. Жахлива статистика кіберзлочинів змушує задуматися про інструменти розслідування хакерських атак і первинного реагування на них. При виникненні подібних ситуацій більшість компаній вважає за краще звертатися за допомогою до профільних фахівців, які займаються розслідуванням комп'ютерних інцидентів і використовують у своїй роботі утиліти з «золотого кейса». Але чи завжди це необхідно?

Як показує практика, немає. Більшу частину інцидентів можна розслідувати внутрішніми силами. Більш того, в деяких випадках навіть при зверненні до фахівців по кіберкриміналістіке (Форензік) потрібно провести первинний аналіз робочих станцій, щоб не втратити час і не дати атакуючому підчистити за собою всі сліди.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ НА КІБЕРІНЦИДЕНТИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

2.1. Аналіз детектування кібератак з штучним інтелектом

Найпопулярнішим завданням в області кібербезпеки є бінарна класифікація, тобто поділ об'єктів на шкідливі і доброякісні з метою виявлення і блокування кібератак. При цьому мається на увазі, що, крім самих класів, ми вже знаємо критерії, за якими проводимо атрибуцію об'єктів. Щоб виробити дані критерії, ми повинні володіти знаннями про загрозу. Іншими словами, методи класифікації дозволяють виявляти відомі типи загроз і вектори атак, але не дають можливості виявляти нову кібератаку, яка не використовує традиційні техніки і не містить відомі нам індикатори.

Крім цього, створення бінарного класифікатора пов'язане з рядом проблем, таких як відсутність розмічених даних і витяг ознак.

Проблема відсутності розмічених даних (заголовок)

Перша проблема якраз і пов'язана з відсутністю великої кількості класифікованих даних, які вже мають мітку (наприклад, об'єкт шкідливий або доброякісний, є індикатором атаки або нормальної активності), які могли б підійти для навчання з учителем.

Наприклад, для того, щоб натренувати нейронну мережу відрізняти котів від собак, необхідно спочатку надати розмічені зображення. Таке маркування зазвичай здійснюється вручну і на великих кількостях даних буде важким. Якщо говорити про кішок і собак, то, на щастя, вже існують готові набори даних від Kaggle, що містять 25 000 класифікованих зображень. Також можна використовувати CAPTCHA, для того щоб користувачі класифікували

зображення при проходженні тесту, що виявляє інтернет-роботів (Internet crawlers) (рис.2.1).

Однак обидва ці варіанти не працюють, коли мова йде про кібератаки. По-перше, техніки кібератак еволюціонують швидше котів і собак, тому модель необхідно регулярно навчати на нових зразках атак. По-друге, звичайних користувачів не можна притягнути до класифікації кіберзагроз зважаючи нетривіальністю даного дії.

Тому більш перспективним є підхід «навчання без учителя» (коли не потрібно попередньо розмічати дані для навчання) або «навчання з підкріпленням» (коли є можливість отримати зворотній зв'язок від експерта).

Рис. 2.1. Приклад CAPTCHA

Проте не варто скидати з рахунків навчання з учителем. Вдалим його застосуванням, наприклад, може бути детектування фішингових посилань.

По-перше, існує база валідованих фішингових посилань на Phishtank.org, куди завантажують нові зразки посилань як антивірусні компанії, так і індивідуальні дослідники. Білі посилання отримати теж нескладно. Для цього можна скористатися сервісом Alexa.com, де є адреси популярних веб-сайтів.

По-друге, різноманітність технік запуску фішингових веб-сайтів обмежена можливостями хостингу і реєстратора доменного імені, і за останні 15-20 років мало що змінилося, хіба що почали більше використовуватися сертифікати. Зловмисники досі реєструють співзвучні атакується сервісу доменні імена на мінімально можливий термін. Хостинг для фішинговою сторінки також вибирається локальний, або використовується зламаний сервер. У більшості атак зазвичай застосовується протокол HTTP без шифрування і сертифікатів. Таким чином, в якості атрибутів досить взяти доменне ім'я, WhoIs-інформацію, геолокацію сервера, тип мережевого протоколу (HTTP або HTTPS) і наявність сертифіката і його параметрів.

Завдання детектування фішингових посилань можна вирішити за допомогою бінарного класифікатора. Причому необов'язково використовувати складний апарат глибоких нейронних мереж (DNN), який вимагає великої кількості даних для якісного навчання. Досить скористатися традиційними інструментами класифікації (дискримінантний аналіз, метод опорних векторів, дерева прийняття рішення, випадковий ліс, регресійний аналіз [передбачення]) або створенням репутації моделі (scoring system) на основі статистичного розподілу атрибутів між двома класами посилань і експертної оцінки.

Розглянемо задачу детектування фішингових посилань на основі наступних атрибутів: реєстратор домену, період реєстрації домену, геолокація хостинг-сервера і наявність захищеного з'єднання з дійсним сертифікатом. Дану задачу я пропоную вирішити на лабораторній роботі своїм студентам, використовуючи ресурс Phishtank.com як джерело класифікованих фішингових посилань. Приклад вибірки посилань з атрибутами і міткою класу (табл. 2.1).

Таблиця 2.1

Вибірки посилань з атрибутами і міткою класу

№	URL	IP address	Registrar	Lifetime	Country	Class
1	[http://]admin.palmariguani.com/...	192.186.205.8	godaddy	2	US	phishing
2	[http://]www.whoes.info/docs/fox/dropbox/	107.180.26.63	godaddy	1	Murrica	phishing
3	[http://]www.apple-id.ldn-app.mobi/apple	208.109.255.48	godaddy	1	US	phishing
4	[http://]v01-apple.co.uk	45.79.129.214	godaddy	1	UK	phishing
5	[https://]www.bth.se/	194.47.131.132	SE Direkt	14	SE	benign
6	[https://]wikipedia.com	208.80.154.238	MARKMONITOR INC.	16	US	benign
7	...	...	...	...	...	...

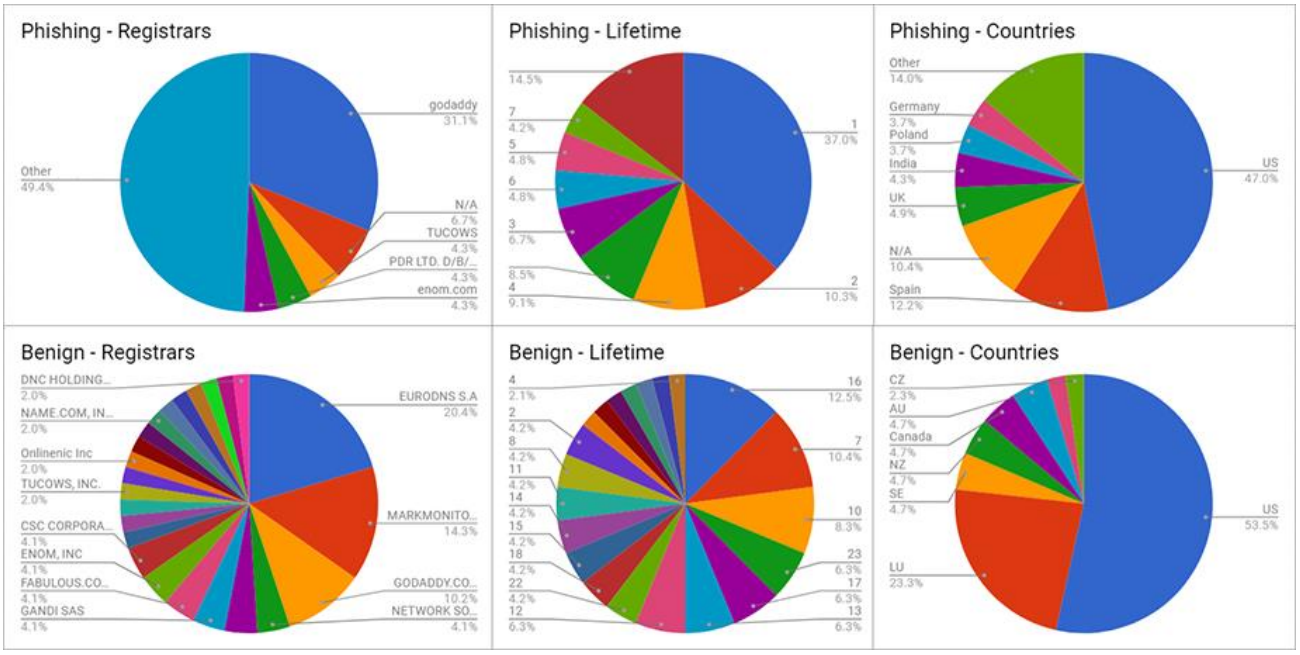

Рис. 2.2. Частота зустрічальності значень трьох атрибутів

Діаграми, що показують частоту зустрічальності значень трьох атрибутів: а) назва реєстратора (Registrar), б) період реєстрації домену (Lifetime), в) геолокація хостинг-сервера (Countries) для фішингових і доброякісних посилань(описание диаграм)

Після частотного аналізу двох вибірок з фішинговими (Phishing) і доброякісними (Benign) посиланнями ми бачимо, що атрибути реєстратора і геолокації буде складно використовувати для бінарної класифікації, так як серед найбільш часто зустрічаються значень є багато збігів. Відмінності за цими двома атрибутам носять більш тонкий характер і можуть бути виявлені на вибірках більшого розміру. Однак атрибут Lifetime, що відповідає терміну, на який реєструється домен, показує, що серед фішингових посилань існує тенденція реєструвати домени на більш короткий термін. Наприклад, 37% фішингових доменів було зареєстровано на 1 рік, на відміну від доброякісних доменів, які зазвичай реєструються на більш тривалий термін - 10 років і довше.

Що ж стосується захищеного з'єднання, то переважна більшість фішингових посилань (96%) не використовують HTTPS-протокол, т. Е. Це один з істотних критеріїв, який можна застосовувати для детектування фішингу. Для HTTPS-посилань можна додатково проводити аналіз сертифіката на основі його атрибутів:

наприклад, ким і кому видано, адреса реєстрації компанії, якій був виданий сертифікат. Хакери можуть реєструвати сертифікати на неіснуючі компанії, як це було у випадку з компанією шифрувальника LockerGoga, файли якого були підписані цифровими сертифікатами, випущеними Sectigo RSA Code Signing CA для фейковий компаній Alina Ltd, Kitty's Ltd., Mikl Limited і AB Simba Limited. Рекомендую до прочитання дослідження Chronicle з цього приводу.

При підготовці вибірки для навчання нам необхідно все строкові значення перевести в категоріальні і закодувати їх числовими значеннями; для категорії можна використовувати порядковий номер. В такому випадку значення атрибута можна буде представити в числовому просторі. Наприклад, для категоріального атрибуту Country створимо новий числовий атрибут Country_code з порядковим номером країни, зустрічається у вибірці (1 - Australia, 2 - Bangladesh, 3 - Canada, ..., 28 - USA).

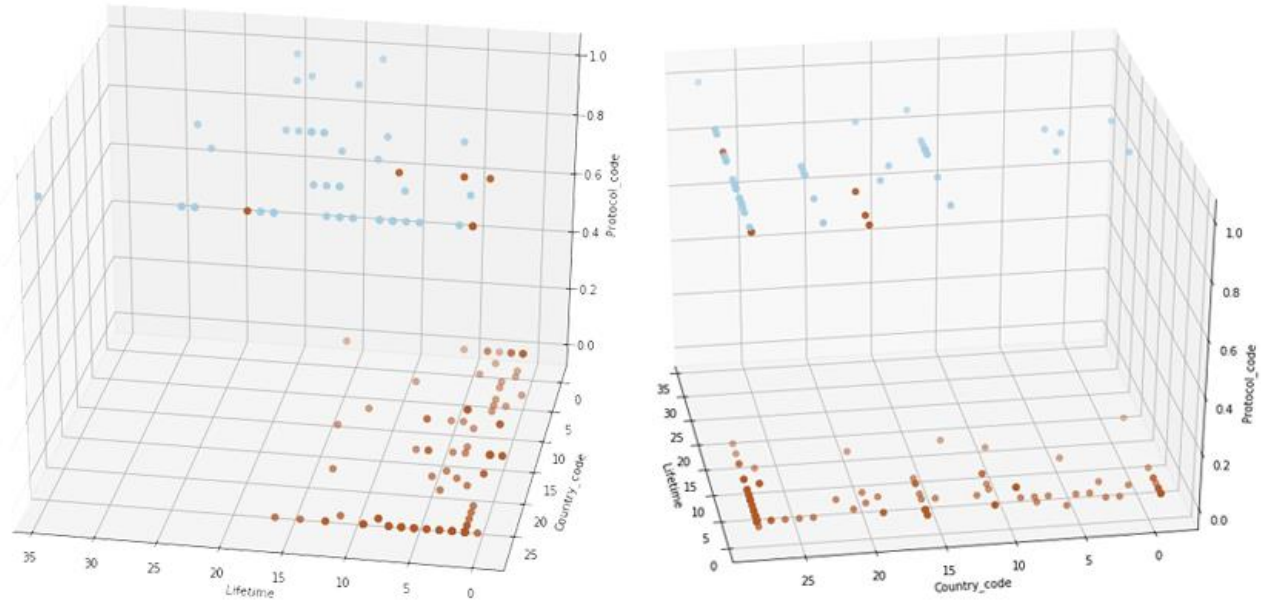

Рис. 2.3. Розподіл фішингових і доброякісних посилань

Розподіл фішингових (помаранчеві точки) і доброякісних (блакитні точки) посилань в залежності від періоду реєстрації (lifetime), геолокації (Country_code) і типу протоколу (Protocol_code: {0 - http, 1 - https}) (опис картинки)

На рис.2.3 видно кілька тенденцій в розподілі даних:

• велика кількість (47% фішингових і 53% доброякісних) IP-адрес знаходиться в США (Country_code = 28);

• переважна більшість фішингових посилань (96%) використовують HTTP-, тоді як всі доброякісні посилання використовують HTTPS-протокол;

• період реєстрації доменів фішингових посилань в цілому істотно менше, ніж у доброякісних посилань. На більшій вибірці ця тенденція буде краще виражена і буде прагнути до 1 року.

А тепер скористаємося методом k - найближчих сусідів (англ. K-nearest neighbors algorithm, k-NN) для класифікації посилань. При класифікації метод привласнює об'єкту клас, який є найбільш поширеним серед k-сусідів даного об'єкта, класи яких вже відомі.

Спершу навчимо нашу модель, після чого побудуємо карту класифікатора, щоб побачити кордон прийняття рішення. Якщо нова посилання потрапить в блакитну зону, то вона буде класифікована як доброякісна, якщо в помаранчеву - як фішингова. Точність класифікатора буде тим вище, чим більше маркованих посилань буде містити тренінгова вибірка. Крім того, можна експериментувати з параметрами моделі, такими як кількість найближчих сусідів, вагова функція, алгоритм знаходження найближчих сусідів і іншими (рис.2.4).

Бінарний класифікатор на основі методу k - найближчих сусідів. Параметри: кількість сусідів k = 5; вагові функції: зліва - uniform (всі крапки в кожній околиці мають однакову вагу) і праворуч - distance (ближчі сусіди точки запиту матимуть більший вплив, ніж сусіди, які знаходяться далі).

Далі навчений класифікатор ми можемо використовувати для детектування фішингових посилань. Наприклад, hxxps: //www.ebay.com.items-checkout.us/item=2328358263481rt=nctrksid=p2328358263481/ (джерело: Phishtank) - посилання, що веде на підроблену сторінку Ebay з наступними атрибутами: домен зареєстрований на 1 рік (27.01 .2019 - 27.01.2020), сервер знаходиться в США, протокол HTTPS, реєстратор NameCheap, Inc. буде задетектірован нашим класифікатором як фішинг. А ось якби домен був зареєстрований не на 1 рік, а на 3, то наш класифікатор визначив би, що сайт доброякісний.

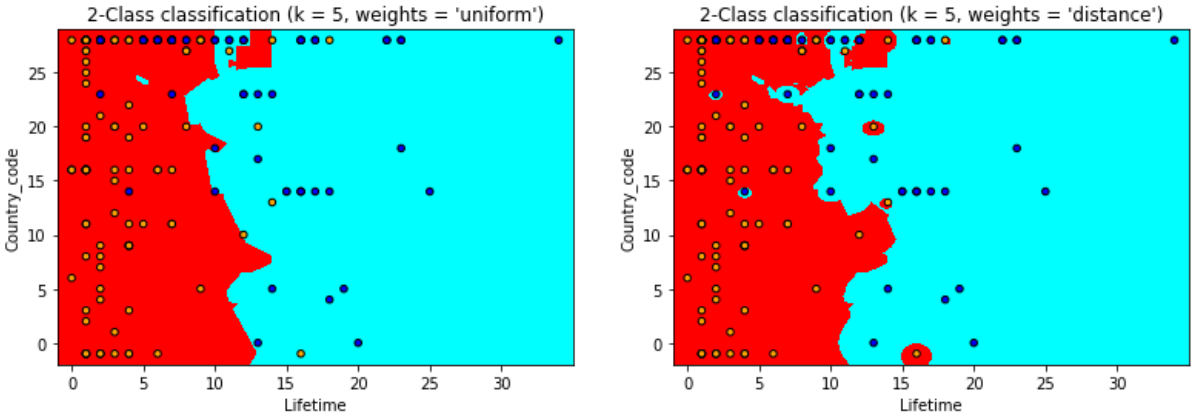

Рис. 2.4. Карта класифікатора

Для оцінки класифікатора необхідно провести його крос-валідацію (перехресна перевірка) на тестовій вибірці з відомими класами. Результатом тестування буде виявлення відсотка помилкових спрацьовувань. Зокрема, для оцінки класифікатора можуть бути використані наступні базові метрики:

• True positive (TP) - кількість фішингових посилань, визначених як фішингові;

• True negative (TN) - кількість доброякісних посилань, визначених як доброякісні;

• False positive (FP) - кількість доброякісних посилань, визначених як фішингові;

• False negative (FN) - кількість фішингових посилань, визначених як доброякісні

І похідні від них:

• True positive rate (TPR) або Recall = TP / (TP + FN);

• True negative rate (TNR) = TN / (TN + FP);

• False positive rate (FPR) = FP / (FP + TN);

• False negative rate (FNR) = FN / (FN + TP);

• Precision або Positive predictive value (PPV) = (TP + TN) / (TP + TN + FP + FN);

• Negative predictive value (NPV) = TN / (TN + FN);

• F-measure - гармонійне середнє між Recall (TPR) і Precision (PPV) = 2 * Precision * Recall / (Precision + Recall).

У контексті завдання виявлення кібератак найбільш важливою є метрика FN / FNR, яка дає кількісну оцінку пропущеним атакам.

Візуалізація і зменшення мірності.

Так як кількість ознак (атрибутів) в моделі часто більше, ніж 2 або 3 (в реальних моделях - 1000 і більше), то виникає питання: як представити об'єкти або спостереження в двох-або тривимірному просторі, щоб побачити закономірності їх розподілу для оцінки можливості подальшої класифікації або кластеризації. Для цих цілей можна скористатися методами зменшення розмірності. Далі ми розглянемо дві техніки - лінійного (PCA) і нелінійного (t-SNE) зменшення розмірності.

Метод головних компонент (англ. Principal component analysis, PCA) здійснює лінійне відображення даних в простір меншої розмірності таким чином, що дисперсія даних в малорозмірних поданні максимизируется.

У нашому випадку зменшення розмірності до двох компонент маємо наступні значення:

• компонента 1: -0.998 x Registrar_code + 0.065 x Lifetime + -0.022 x Country_code + 0.006 x Protocol_code

• компонента 2: 0.020 x Registrar_code + -0.035 x Lifetime + -0.999 x Country_code + -0.005 x Protocol_code

Ми бачимо, що основний внесок в компоненту 1 вносить реєстратор домену, а в компоненту 2 - країна, де знаходиться сервер. Це можна пояснити тим, що обидві ці величини є категоріальним і після кодування з використанням порядкового номера значення атрибута мають велику дисперсію; розкид значень в інтервалах значень атрибутів (Registrar_code: [1,92], Country_code: [1, 28], Lifetime: [1,34], Protocol_code: [0,1]). В даному випадку варто поекспериментувати з алгоритмами кодування категоріальних даних, наприклад використовувати one-hot-кодування.

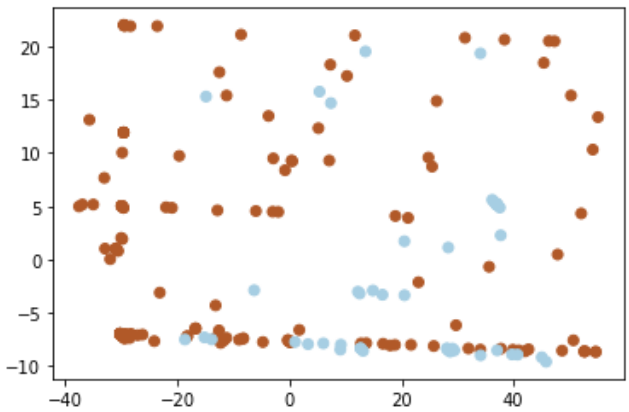

Рис. 2.5. застосування техніки PCA

В двовимірному просторі після застосування техніки PCA (фішингові посилання - помаранчеві точки, доброякісні посилання - блакитні точки) (опис картинки)

На рис. 2.5 складно виділити окремі групи доброякісних і фішингових посилань. Дана техніка для нашого випадку неефективна.

Іншим алгоритмом є стохастичне вкладення сусідів з t-розподілом (англ. T-distributed Stochastic Neighbor Embedding, t-SNE), що представляє нелінійну техніку зменшення розмірності даних.

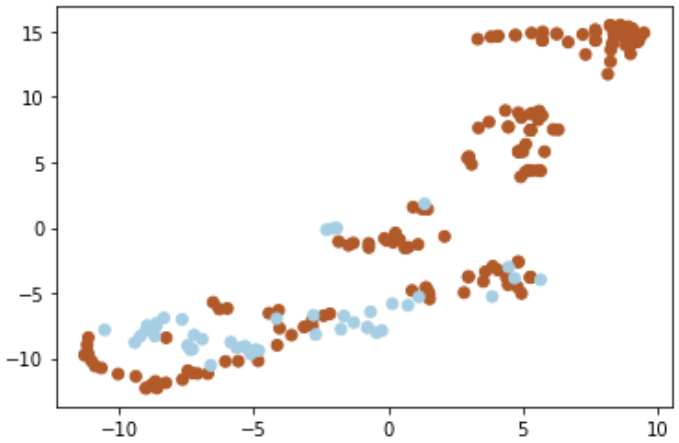

Рис. 2.6. Застосування стохастичне вкладення сусідів

В двовимірному просторі після застосування техніки t-SNE (фішингові посилання - помаранчеві точки, доброякісні посилання - блакитні точки).

В цьому випадку ми вже можемо побачити скупчення посилань різних класів; це говорить про те, що існують ознаки або їх сукупність, значення яких можна використовувати для визначення приналежності об'єктів до одного з класів.

Припустимо, що у нас немає міток класів (фішингові і доброякісні) для інтернет-посилань. У такому випадку ми можемо використовувати навчання без учителя, а саме кластерний аналіз. Кластеризація дозволяє згрупувати об'єкти невідомих класів по спільності ознак.

Для цього скористаємося популярним методом кластеризації k-середніх (англ. K-means). K-means прагне мінімізувати сумарне квадратичне відхилення точок кластерів від центрів цих кластерів. У нашому випадку кількість кластерів дорівнює двом. Використовуючи техніку t-SNE для проекції даних на двовимірну площину, отримуємо такі візуалізовані результати.

Отримані кластери можна порівняти з розміченими даними на рис.2.7 для того, щоб отримати уявлення про точність кластерного аналізу.

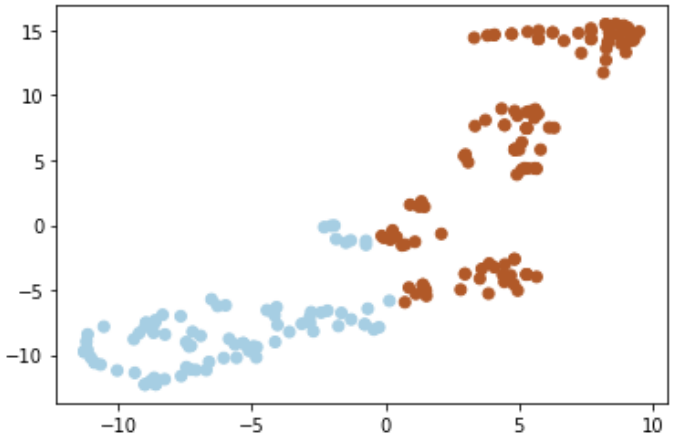

Рис. 2.7. Техніка SNE

В двовимірному просторі після кластерного аналізу з допомогою методу K-means.

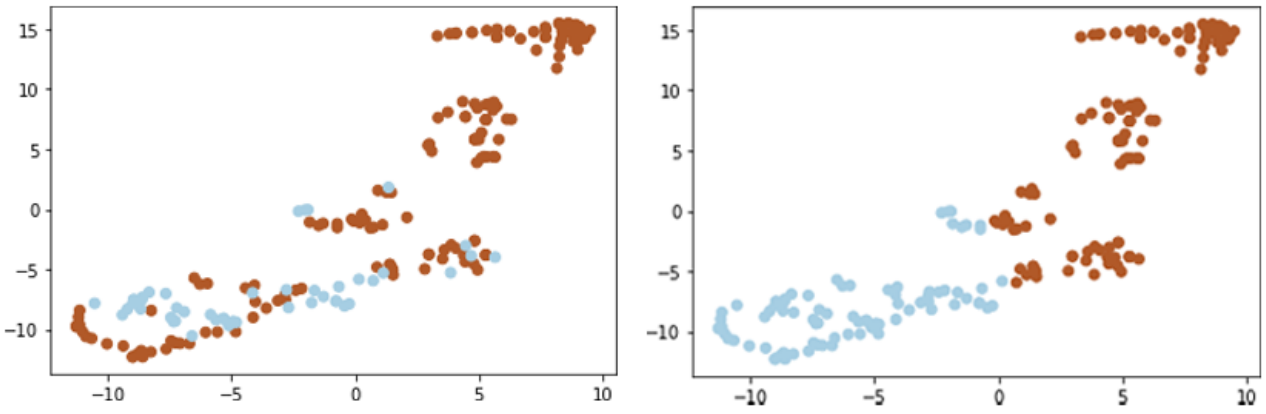

Рис. 2.8. Порівняння кластерного аналізу

Навчальна вибірка з позначеними знаками класів (зліва) і після кластеризації (праворуч) (опис)

Більш точну оцінку ефективності кластеризації можна отримати, використовуючи описані вище метрики: TPR, TNR, FPR, FNR, PPV, NPV, F-measure.

TP = 110, TN = 41, FP = 7, FN = 44;

TPR (Recall) = 71%;

TNR = 85%;

FPR = 15%;

FNR = 29%;

PPV (Precision) = 0.75;

NPV = 0.48;

F-measure = 0.73.

Очевидно, що такий точності класифікатора недостатньо для самостійного використання в продакшен-системах. Однак, з огляду на той факт, що у нас не було міток класів і ми не навчали нашу модель, це хороший результат. Даний класифікатор може бути затребуваний як додатковий механізм в рамках евристичного підходу для виявлення підозрілих посилань, на які слід звернути увагу і, можливо, піддати глибшого аналізу або скануванню іншими сервісами, наприклад Phishtank або Virustotal. Також можливо вдатися до кластеризації для

допомоги в маркуванні об'єктів, які в подальшому, після перевірки експертом, будуть використовуватися для навчання моделі класифікатора (навчання з учителем) або для детерминистических методів - пошуку однозначного відповідності з виявленою фішинговою посиланням.

Висновки

Ми розглянули основні парадигми ІІ, взаємні відносини МО і ШІ, а також на прикладі задачі детектування фішингових посилань досліджували можливості навчання з учителем і без нього, попутно торкнувшись техніки зменшення розмірності і візуалізації даних.

Навчання без вчителя, незважаючи на невисоку точність, зараз є найбільш перспективним напрямком наукових досліджень. Такі моделі не вимагають розмічених даних і тому мають великий потенціал для застосування, в тому числі в області кібербезпеки.

Одним з таких перспективних напрямків є детектування аномалій без вчителя. Сьогодні цей підхід активно впроваджується в системи моніторингу та управління подіями інформаційної безпеки (англ. Security Information and Event Management, SIEM) і дозволяє виявляти аномальну активність користувачів і систем, яка може сигналізувати про цільову кібератаці на організацію.

Цікавим, на мій погляд, також є дослідження можливостей застосування генетичних алгоритмів (англ. Genetic Algorithms) і навчання з підкріпленням (англ. Reinforcement Learning) на додаток до популярних Fuzzing і Symbolic Execution для тестування безпеки програмних продуктів (англ. Security Testing) і виявлення вразливостей в них (англ. Vulnerability Testing).

Для детектування і аналізу шкідливих програм (англ. Malware) може виявитися корисним Smart Pattern Matching.

І нарешті, всемогутній Deep Learning, який поки ще не набув широкого застосування в кібербезпеки, проте вже успішно використовується в суміжних областях, зокрема, в медіабезопасності для детектування фейковий новин [14].

2.2. Аналіз можливостей системи IBM QRadar SIEM для розслідування кіберінцидентів в корпоративній інформаційній системі

Збір даних і нормалізація: забезпечується збір даних (як подій ІБ, так і системних подій) від різноманітних джерел: технічні засоби інформаційної безпеки (міжмережеві екрани всіх типів, системи запобігання вторгнень, антивіруси, системи захисту від спаму, системи захисту від витоків даних, системи попереднього виконання програм, контролю цілісності і т. д.), сервери, прикладні системи і т. д.

Корреляция данных: зіставлення і пошук по атрибутам, групування і індексування за певними ознаками. По суті кореляція є ключовою функцією SIEM, яка видає на виході список корелюється подій;

Сповіщення: перевірка списку корельованих подій з метою виявити інциденти ІБ і виконати сповіщення за даними інцидентів. Можлива як індикація на консолі управління SIEM, так і автоматизоване повідомлення по спрацьованим кореляційним правилам.

Панелі візуалізації (dashboards): графіки різних типів і форматів, таблиці, списки і інша візуалізація щодо поточних подій і інцидентів. Візуалізація в значній мірі впливає на загальне сприйняття продукту і є важливим елементом процесу Incident Monitoring / Tracking.

Зберігання даних: зберігання даних протягом заданого періоду часу. Необхідно для ретроспективного аналізу, розслідувань інцидентів, експертиз. Більшість сучасних SIEM обробляють і зберігають як сирі події (до процесу здійснення розпізнавання функціональних полів події (анг. - parsing), так і нормалізовані події (події з розпізнаними полями).

Пошук і аналіз: контекстний пошук в рамках розслідувань інцидентів і експертиз. Важливо відзначити, що пошук в сирих і нормалізованих події може істотно відрізнятися.

Звітність: створення звітів, що настроюються з метою періодичного інформування служби ІБ про поточні події, інциденти, трендах. Як правило, звіти

можуть розвантажуватися і використовуватися в рамках комплексних звітів служб ІБ.

Склад і реалізація істотно залежать від архітектури рішення, розміру впровадження, географічного розподілу системи, параметрів продуктивності. Як правило, для реалізації всіх базових функцій в SIEM повинні бути присутні кілька основних компонентів.

Колектори: відповідають за збір сирих подій. Можуть підтримувати масу різних протоколів і сервісів: Syslog, Windows Event Forwarding, SDEE, SNMP Trap, клієнтів баз даних (MSSQL, Oracle і т. Д.) Та інші специфічні сервіси від різних виробників. Сам збір подій може відбуватися як в пасивному режимі (наприклад, syslog), так і в режимі "на вимогу". Колектор найчастіше відправляє нормалізовані події в коррелятор, а сирі події відправляються в сховище даних. У різних реалізаціях від різних виробників схема взаємодії колектора з іншими компонентами може відрізнятись.

Сховище даних: відповідає за зберігання сирих подій. Можливі реалізації зі зберіганням нормалізованих подій.

Коррелятор: забезпечує функції обробки і кореляції нормалізованих подій. Можлива реалізація контекстного пошуку сирих подій, що знаходяться в сховищі.

Консоль управління: відповідає за управління, настройку та візуалізацію. При цьому, в ряді випадків, функція візуалізації може виконуватися окремим компонентом. Згадані SIEM другого покоління можуть містити також додаткові компоненти: збір Flow і SPAN-трафіку, BI-компоненти, TI-модуль, модулі управління політиками ІБ.

Як було сказано вище, на практиці архітектура впровадження має визначальний вплив на кількість компонент і їх реалізацію. Наприклад, в малих реалізаціях майже всі функції можуть бути виконані на одному апаратному пристрої, тоді як масштабування передбачає максимальне поділ.

На сьогоднішній день складно переоцінити роль SIEM в світі ІБ. Фактично, це центральний елемент будь-SOC-інфраструктури. Можна сказати точно, що без SIEM неможливе ефективне функціонування жодної комплексної системи ІБ.

Завдання SIEM номер один - реєстрація інцидентів в режимі Real-Time. Завдання SIEM номер два - надати зручний і функціональний інструмент для ретроспективного аналізу інцидентів, розслідування інцидентів.

Сучасний SIEM, по суті, вже повинен містити в собі Big Data технології, обробні події ІБ як якийсь інтенсивний потік телеметрії. Від SIEM потрібно як швидкість, так і зручність - тому що це основний інструмент аналітики ІБ, призначений для розслідування інцидентів, пошуку слідів націлених атак (Threat Hunting).

Тренди розвитку SIEM йдуть в сторону додавання функцій Machine Learning і поведінкового аналізу, що дозволяє передати на відкуп автоматизації все більше і більше рутинних завдань Incident Monitoring, Forensic, Investigation. На практиці це дозволить виявляти не тільки існуючі вручну інциденти, але і наблизитися до автоматизації процесу створення правил кореляції, що є ключовою і найскладнішим завданням при настройці і підтримці SIEM (особливо на великих впроваджень).

2.3. Аналіз використання технології Qradar Advisor with Watson

В нашу інтернет-епоху інформаційна безпека є наріжним каменем. Цьому можна не дивуватися, оскільки даних в мережі надзвичайно багато, а користувачів - мільярди. Якщо зловмисники отримають доступ хоча б до малої дещиці всієї цієї інформації, можна чекати біди (що, власне, відбувається з завидною регулярністю). Звичайно, експерти з безпеки працюють, різні компанії випускають інструменти, що дозволяють, теоретично, уберегтися від втручання зловмисників у нормальний робочий процес.

Але, незважаючи на вжиті заходи, проблеми найчастіше виникають навіть у самих, здавалося б, захищених компаній і організацій. Нещодавно стало відомо, наприклад, що через масове поширення в мережі вірусу WCry в деяких областях Росії навіть довелося скасувати видачу водійських прав. Цей вірус скомпрометував багато комп'ютерів, які без розблокування практично неможливо використовувати.

Що буде, якщо мережі досить великої комерційної компанії заблокує вірус? Така компанія зазнає багатомільйонних, а то і мільярдні збитки. Так воно і є, зараз зупинити епідемію WannaCry вдалося тільки дивом, а збитки ще ніхто не підраховував.

Стандартні інструменти захисту не завжди справляються з загрозою, але когнітивна система може значно все спростити, керуючи кібербезпекою підприємства. У корпорації IBM є такий продукт, це сервіс Watson for Cyber Security. Детальніше про це - нижче.

На даний момент фахівці з інформаційної безпеки зафіксували десятки тисяч вразливостей в різному програмному забезпеченні. Кожен день з'являється нове ПЗ, виявляються нові «дірки» в існуючому програмному забезпеченні, зловмисники випускають віруси, створюють експлоїти, займаються зломом звичайних і корпоративних мереж. Зрозуміло, що фахівці з кібербезпеки не дрімають. Кожна виявлена уразливість ретельно документується, часто, така інформація викладається у відкритому доступі. Але це не завжди допомагає, оскільки кожен місяць автори публікують мінімум 60 000 статей, що мають відношення до цієї сфери. Зрозуміло, що встежити за таким потоком даних нездатний ніхто. Вірніше, ніхто, крім Watson - когнітивна платформа здатна засвоювати тисячі і тисячі документів в одиницю часу. Практично всі ці дані безструктурні, багато матеріалів ніяк один з одним не пов'язані, хоча і можуть містити схожі теми.

В інформаційній безпеці, як ніде, потрібно використання машинного навчання і обробка природної мови. Ці технології, як і інші з ними пов'язані, стають все більш досконалими з плином часу. Комп'ютерні системи навчаються на прикладі кожної знайденої уразливості або проблеми, стаючи все більш досконалий в роботі з зовнішніми і внутрішніми інформаційними загрозами.

На основі сервісу Watson for Cyber Security працює один з продуктів платформи IBM QRadar - IBM Qradar Advisor with Watson.

Когнітивна система IBM Watson допомагає аналітикам, які займаються виявленням загроз, справлятися зі своєю роботою ефективніше і якісно. Ніхто не

може отримати всю необхідну інформацію про проблему, особливо про складну, за кілька секунд. А ось комп'ютерна система Watson може, і робить це. Вона визначає потенційну загрозу, шукає інформацію по ній, аналізує те, що відбувається і діє по необхідності.

Всі дані зберігаються, так що їх може вивчити як людина, так і сама когнітивна система згодом. IBM Watson може, наприклад, виявивши якусь аномалію в корпоративній мережі, дістатися до суті проблеми, причому дуже швидко. В результаті ця проблема не встигає стати актуальною, загроза знищується ще «на підході». Дані надаються групі технічної підтримки, яка діє далі, грунтуючись на даних, наданих Watson. Все це відбувається швидко, система працює з високим ступенем точності.

Робота IBM Qradar Advisor with Watson ведеться в режимі 24/7/365. Вона складається з чотирьох ключових елементів:

1. Виявлення інциденту і виявлення його причини. При цьому когнітивна система активно працює з даними моніторингу роботи мережі, накопичених Qradar;

2. Далі йде пошук по базі даних самої когнітивної системи, для виявлення інформації, яка відноситься до виявленої аномалії або події;

3. Далі Qradar Advisor відправляє інформацію про проблему в Watson for Cyber Security, для фіксування цих даних і вивчення проблеми;

4. Йде ідентифікація загрози і пошук підходящої стратегії боротьби з нею.

До речі, в 2015 році інститут Понемона проводив вивчення особливостей роботи різних компаній з QRadar. В рамках цього дослідження було проведено опитування. Представників компаній, які погодилися взяти участь в опитуванні, запитали, чи працювали вони з додатковими сервісами з мережевої безпеки після впровадження Qradar. 70% опитаних відповіли, що ні, причому 62% заявили, що якби хотіли, без проблем змінили б продукт, але такого бажання не виникало. 43% опитаних заявили, що відчули ефект від роботи з сервісом вже через кілька днів, для 27% цей ефект проявився протягом тижня.

В цілому, гідності QRadar, включаючи і когнітивний сервіс, можна виділити в наступні пункти:

• Єдина архітектура для аналізу журналів, мережевих потоків, пакетів, вразливостей, даних про користувачів і ресурсах

• Аналіз кореляції в реальному часі з використанням Sense Analytics для виявлення найбільш серйозних загроз, атак і вразливостей

• Розстановка пріоритетів і виділення найважливіших інцидентів серед мільярдів одиниць даних, одержуваних щодня

• Прогнозний аналіз наявних ризиків, викликаних некоректним настроюванням пристроїв і відомими уразливими

• Автоматичне реагування на інциденти

• Автоматичне виконання нормативних вимог за рахунок можливостей збору даних, визначення їх кореляції і складання звітності

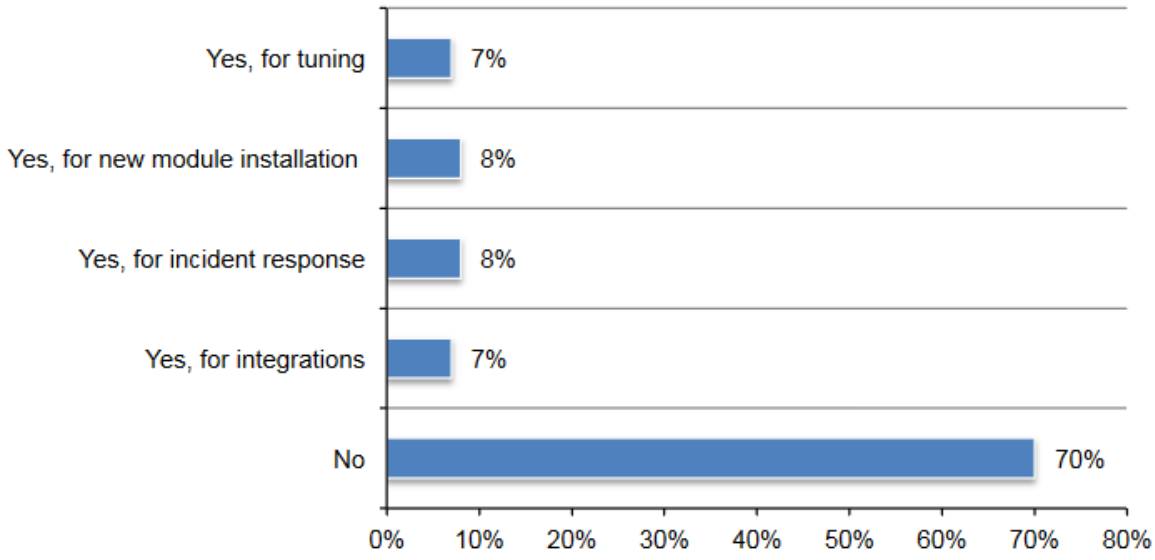

Рис. 2.9. Статистичні дані опитування

За оцінкою інституту Понемона, звичайна компанія витрачає понад 20 000 в рік на роботу з мережевими погрозами, як зовнішніми, так і внутрішніми. Це величезна кількість часу, і його можна заощадити, якщо автоматизувати всі процеси моніторингу.

Watson for Cyber Security оперує в своїй роботи даними з 100 000 задокументованих вразливостей ПЗ, що містяться в базі даних IBM X-Force

Exchange. Також в розпорядженні когнітивної системи більше 10 000 різних документів і 700 000 записів в блогах фахівців з інформаційної безпеки, що публікуються щороку. У разі необхідності всі ці дані можна швидко структурувати і отримати необхідну інформацію з певної тематики. Структуровані дані, сформовані Watson for CyberSecurity, надходять в сервіс IBM QRadar, про що вже говорилося вище. Якщо говорити про ефективність роботи такої системи, то вона може аналізувати тисячі інцидентів в день, сортуючи помилкові спрацьовування і актуальні проблеми з безпекою.

Незабаром Watson for Cyber Security стане частиною нової платформи Cognitive Security Operations Centre (SOC), яка остаточно об'єднає когнітивні технології та операції в сфері мережевої безпеки. Ключовим елементом платформи є IBM BigFix Detect. Це рішення, що дозволяє відстежити атаку, використовує своєрідну «машину часу» для виявлення початкової точки, де все почалося. Для кінцевого користувача це означає можливість швидко, дуже швидко відповідати на виникаючі загрози, включаючи локальні мережі та «хмари». Другі компоненти SOC - це IBM Security, X-Force Exchange і i2. Доступ до цієї уніфікованої платформі IBM планує надавати в якості сервісу, який так і називатиметься SOC-as-a-Service[9].

Підрозділ IBM Security представило рішення Watson for Cyber Security, першу в галузі доповнену інтелектуальну технологію, розроблену для управління когнітивними центрами інформаційної безпеки (security operations centers, SOC).

Протягом минулого року система Watson навчалася мови кібербезпеки і опрацювала понад 1 млн документів по цій темі. Сьогодні система здатна допомогти аналітикам з питань безпеки розібратися в тисячах звітів, підготовлених на природній мові, які раніше були недоступні звичайним інструментам інформаційної захисту.

Згідно з дослідженням IBM, команди по забезпеченню інформаційної безпеки щодня фільтрують понад 200 тис. Інцидентів в системі захисту. В результаті понад 20 тис. Годин на рік йде на обробку помилкових погроз. Необхідність впровадження когнітивних технологій в центри інформаційної

безпеки стоїть особливо гостро, оскільки протягом наступних п'яти років кількість інцидентів в системі захисту збільшиться вдвічі. Також зросте рівень регулювання сфери по всьому світу.

Рішення Watson for Cyber Security буде інтегровано в нову платформу IBM Cognitive SOC, об'єднавши передові когнітивні технології та операції в системі безпеки. Це дозволить реагувати на загрози, що виникають на кінцевих пристроях, в мережі, у окремих користувачів і в хмарі. Центральним компонентом платформи є IBM QRadar Advisor with Watson, перший інструмент, підключений до бази инсайтов з кібербезпеки Watson. Новий додаток вже використовують компанії Avnet, Університет Нью-Брансвік, Sopra Steria і 40 інших організацій по всьому світу. Воно допомагає розслідувати інциденти в системі безпеки, які проводять аналітики.

IBM також інвестувала в проведення досліджень з метою включити в свою мережу X-Force Command Center такі когнітивні інструменти, як керований системою Watson чат-бот. Це рішення зараз використовується для взаємодії з клієнтами IBM Managed Security Services. IBM також запустила новий дослідницький проект під кодовою назвою Havyn. Це перший голосовий помічник в області безпеки, ефективно використовує здатність системи Watson вести діалог. Він може реагувати на усні команди і розуміти природну мову аналітиків з безпеки.

«Сучасні витончені кібератаки використовують безліч каналів з метою приховати свої активності. Нашим фахівцям з безпеки дуже складно виявити ці загрози у величезних масивах даних, пов'язаних з інформаційною захистом, - сказав Шон Валкамп, директор з інформаційних технологій Avnet. - Система Watson перешкоджає спробам приховати інформацію завдяки швидкій обробці великої кількості потоків даних. Потім вона порівнює цю інформацію з відомостями про останні кібератаки і надає більш цілісну картину загроз. Watson протягом декількох хвилин створює звіти по цим загрозам, що дозволяє істотно скоротити кількість часу між виявленням потенційного інциденту і відповідної реакції команди по забезпеченню безпеки».

2.4. Когнітивний центр інформаційної безпеки IBM

Оскільки команди з питань безпеки вдосконалюють свої стратегії і тактику боротьби з кіберзлочинністю, впровадження когнітивних технологій в процеси систем безпеки вкрай важливо. У недавньому дослідженні IBM відзначається, що сьогодні тільки 7% професіоналів в сфері інформаційної безпеки використовують когнітивні інструменти. Однак, відповідно до очікувань експертів, цей показник збільшиться в три рази через 2-3 роки

Платформа IBM Cognitive SOC надає когнітивні технології аналітикам з питань безпеки, дозволяючи їм більш ефективно ліквідувати прогалини в області збору інформації і діяти оперативно і точно. У додатку IBM QRadar Advisor with Watson аналітики з питань безпеки використовують когнітивні можливості для проведення розслідувань інцидентів і відновлення даних через інтелектуальну платформу з безпеки IBM QRadar. Рішення допомагає виявити причини потенційних загроз, використовуючи можливості Watson по обробці природної мови в блогах з безпеки, на сайтах, в наукових роботах та інших джерелах. Воно співвідносить отримані результати з даними про погрози витоку секретної інформації та про інциденти в системі безпеки з QRadar. В результаті кількість часу, необхідне на розслідування інцидентів в сфері безпеки, зменшується з кількох тижнів і днів до декількох хвилин.

«Cognitive SOC допоможе замовникам отримати перевагу в боротьбі зі зростаючим числом кібершахраїв і погрозами нового покоління, - сказав Денис Кеннел, віце-президент з розвитку і технологій IBM Security. - Наші інвестиції в проект Watson for Cyber Security всього за один рік дали поштовх розвитку кількох інноваційних розробок. Поєднання унікальних здібностей людини і машинного інтелекту стане найважливішим елементом нового етапу боротьби з найсучаснішими методами кіберзлочинів ».

Для розширення можливостей Cognitive SOC на кінцевих пристроях, IBM Security також анонсувала рішення для виявлення і реагування (EDR) під назвою IBM BigFix Detect. Воно дозволяє організаціям отримати повний огляд постійно

мінливого статусу загроз для кінцевих пристроїв і в той же час подолати розрив між виявленням шкідливого поведінки і відновленням. BigFix Detect відкриває доступ до практичного використання EDR, дозволяючи аналітикам з питань інформаційної безпеки бачити, розуміти і реагувати на загрози в кінцевих точках мережі за допомогою єдиної платформи. Додаток також забезпечує адресне відновлення на піддалися атаці кінцевих точках мережі підприємства за лічені хвилини.

Використовуючи можливості комбінування і автоматизації платформи IBM Resilient Incident Response Platform (IRP) замовники можуть на основі висновків і цінних відомостей від SOC здійснювати функції отримання, відновлення і міграції даних. IBM Cognitive SOC також об'єднує інші технології IBM Security, включаючи i2 для пошуку кіберзагроз та IBM X-Force Exchange.

Когнітивні сервіси та інновації в сфері безпеки.

IBM допоможе замовникам розробляти, створювати і управляти когнітивними центрами безпеки по всьому світу за допомогою IBM Managed Security Services. За останні п'ять років IBM побудувала більше 300 центрів безпеки для замовників з різних галузей, в тому числі сфер споживчих товарів, роздрібної торгівлі, банківської справи та освіти. Клієнт може вибрати, чи буде центр захисту створено IBM на території підприємства або він буде управлятися віртуально за допомогою IBM Cloud як частина мережі IBM X-Force Command Center.

Глобальна мережа центрів IBM X-Force Command Centers використовує когнітивні можливості IBM. Зокрема, QRadar Advisor with Watson дозволяє прискорити процес розслідування інцидентів безпеки. Іншим перспективним кейсом є науково-дослідний проект з кодовою назвою Havyn, який додає голосові можливості до когнітивним центрам безпеки. Мета Havyn полягає в створенні голосового помічника з питань безпеки, який зміг би взаємодіяти з аналітиками на такі теми, як оновлення інформації про загрози в режимі реального часу або дані про засоби забезпечення безпеки організації.

Проект Havyn використовує Watson API, BlueMix і IBM Cloud, щоб забезпечити оперативні відповіді на голосові запити і команди, грунтуючись на

інформації про систему безпеки з відкритих джерел, в тому числі IBM X-Force Exchange, а також даних за минулі періоди часу і інструменти замовника . Наприклад, Havyn може надати аналітикам в сфері безпеки оновлену інформацію про нові загрози, які з'явилися останнім часом, і рекомендації щодо дій для відновлення. Проект в даний момент тестують кілька дослідників і аналітиків в рамках IBM Managed Security Services. Watson вже щодня взаємодіє з замовниками в форматі чат-бота, який доступний в мережі IBM's X-Force Command Center, обробної більше трильйона інцидентів безпеки в місяць. Таким чином, замовники можуть задати питання Watson про статус системи безпеки або конфігураціях мережі. Наприклад, можна запитати у Watson про конкретний пристрій або тікет звернення. Інструмент також здатний виконувати команди від замовників IBM Managed Security Systems, зокрема, зробити переадресацію звернення іншому власнику[10].

3 ТЕХНОЛОГІЇ РОСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ ЗА ДОПОМОГОЮ QRADAR ADWISOR WATSON

3.1. Аналіз кіберінцидентів

Останнім часом збільшення центрів безпеки в певній мірі не можуть задовільнять вимоги цілковитого захисту замовників з різних галузей від не передбачуваних кіберінцидентів, які безпосередньо можуть впливати на роботу підприємств, установ та інших споживачів.

Використовуючи дані зібрані «Центром стратегічних та міжнародних досліджень», який вивчає як швидко змінюються технології та кібербезпека і як вони впливають на світ у двадцять першому столітті.

На цій часовій шкалі зафіксовані значні кіберінціденти з 2012 року. На ній зосереджені кібератаки на урядові установи, оборонні та високотехнологічні компанії або на економічних злочинах з втратами понад мільйон доларів[11].

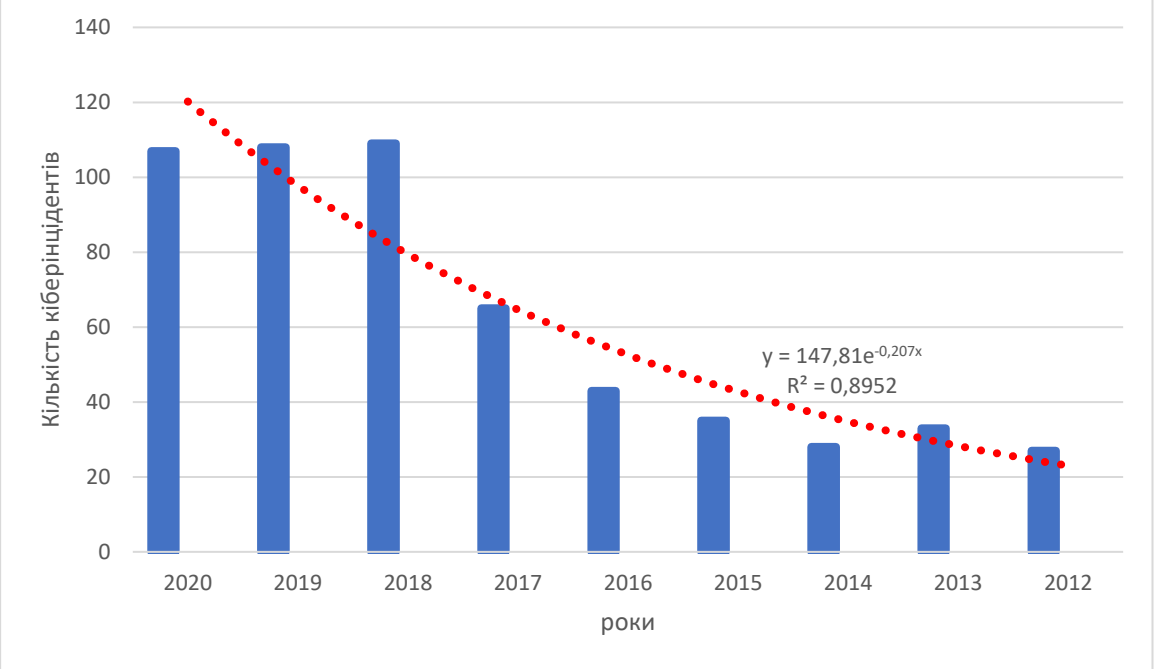

Рис. 3.1. Значні кіберінціденти 2012-2020 рр.

Як видно з рис.3.1, тенденція збільшення кіберінцідентів спостерігається останні 3 роки, що можна пов’язати із збільшенням інформатизації систем.

По відношенню до кількості кіберінцідентів 2020 року в порівнянні з 2012 роком їх кількість збільшилася у 4 рази.

За збільшення проглядається екпотенціальний характер, який описується рівнянням виду $y = 147{,}81e^{-0{,}207x}$

Враховуючи різке збільшення кібер інцидентів в інформаційному просторі, є важливою задачею вчасно їх виявити та знайти шляхи знешкодження. Тому наявність SIEM системи з її можливостями спрощує роботу фахівця інформаційної безпеки завдяки централізованому збору даних з різних джерел.

3.2 Технологія розслідування кіберінцидентів з використання Qradar Adwisor Watson

Watson може приймати та аналізувати великі дані (як структуровані, так і неструктуровані) та виявляти нові закономірності та уявлення за лічені секунди. Унікальне поєднання трьох можливостей відрізняє IBM Watson від інших систем:

- природна обробка мови, яка допомагає зрозуміти складність людського мовлення та письма як як засобу взаємодії з користувачем, так і як джерела даних,

- вироблення та оцінка гіпотез шляхом застосування передової аналітики для зважування та оцінки групи відповідей на основі лише відповідних доказів,

- на основі фактичних даних, що базуються на результатах, щоб бути розумнішими з кожною ітерацією та взаємодією.

Watson є додатком до Qradar. Для того щоб розпочати роботу з виявлення кіберінциденту потрібно зайти на сторінку порушень Qradar.

На сторінці порушень в Qradar вибрати одне з порушень для аналізу (рис. 3.2).

Рис. 3.2. Сторінка порушень в інтерфейсі Qradar

Далі ми переходимо на сторінку вибраного порушення і бачимо детальну інформацію по ньому.

Для початку аналізу порушення с допомогою Watson необхідно натиснути кнопку «Investigate».

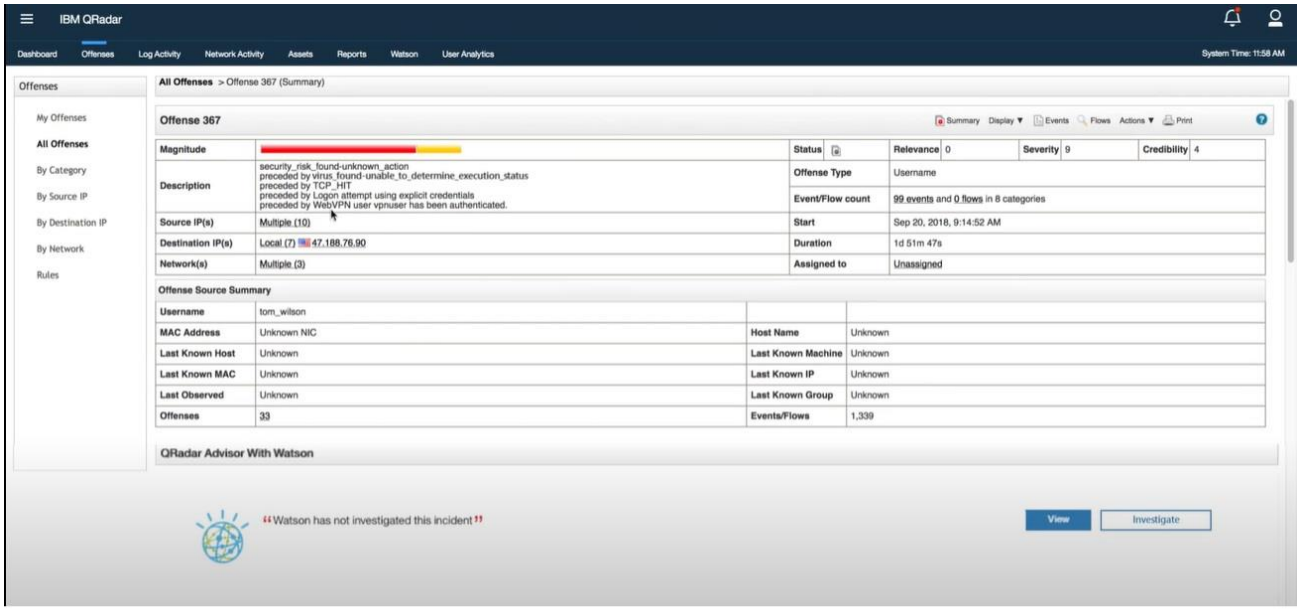

Рис. 3.3. Порушення в інтерфейсі Qradar

Перший крок сбір логів із SIEM системи які мають зв’язки з даним порушенням або об’єктами які були в ньому замічені.

Рис. 3.4. 1 крок аналізу Watson

Другий крок наповнення зібраною інформацією.

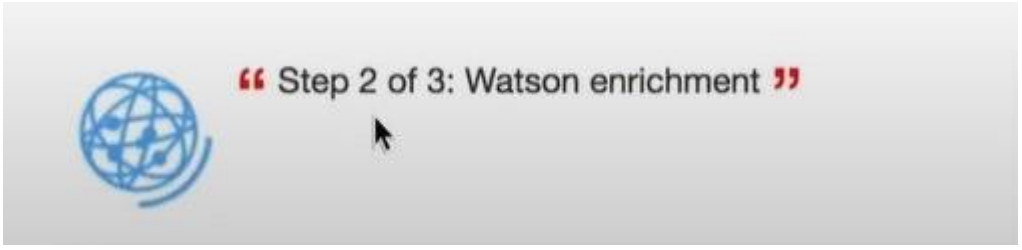

Рис. 3.5. 2 крок аналізу Watson

Далі ми бачимо короткий опис зібраної інформації по порушенню,

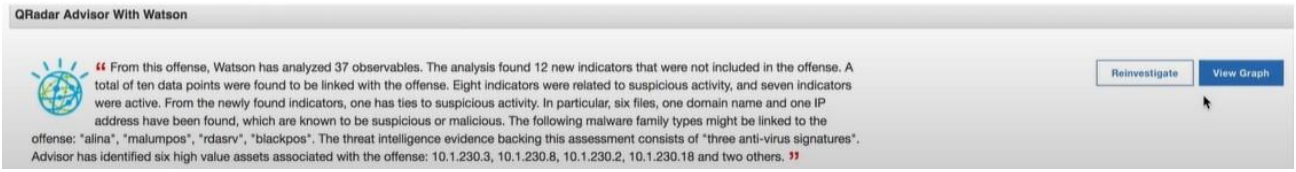

Рис. 3.6. Опис аналізу

після чого натискаємо кнопку «View Graph» і на екрані виводиться повний графік, на якому відображаються користувачі, IP – адреса, назва або hash файлів, URL та зв’язки між ними.[8]

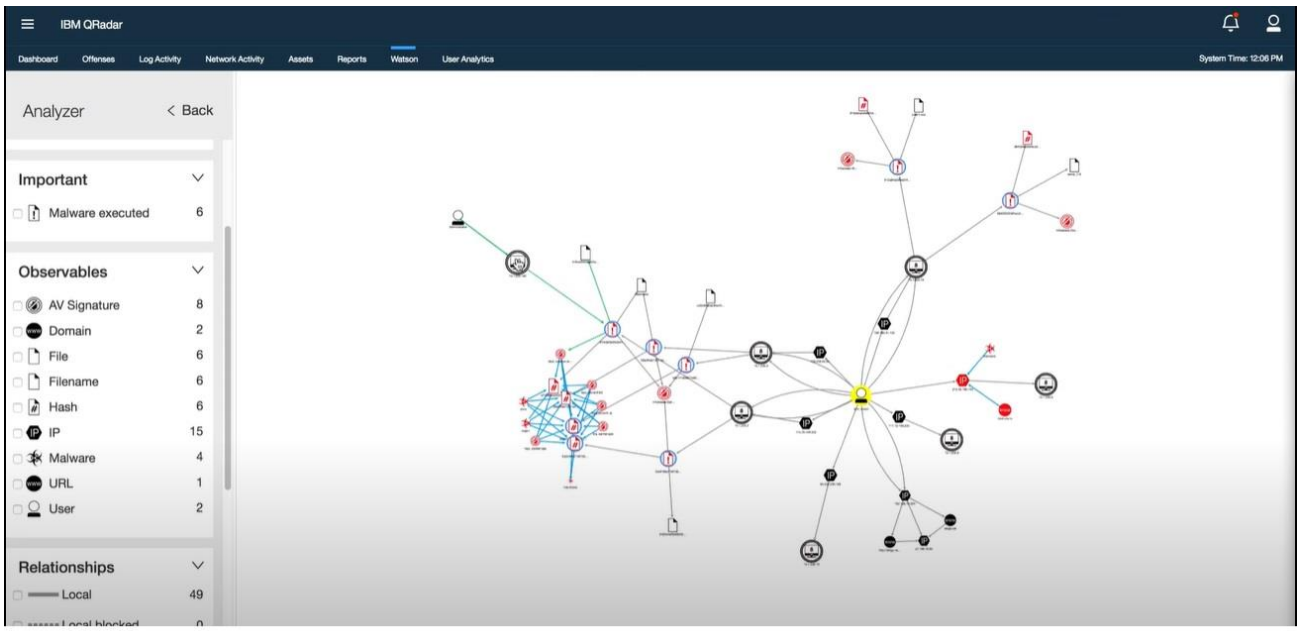

Рис. 3.7. Детальній графік Watson

Натискаючи на графіку ми можемо побачити про них детальну інформацію:

- рівень загрози (low, medium, high);
- опис загрози;
- інформацію про джерело загрози;[12]

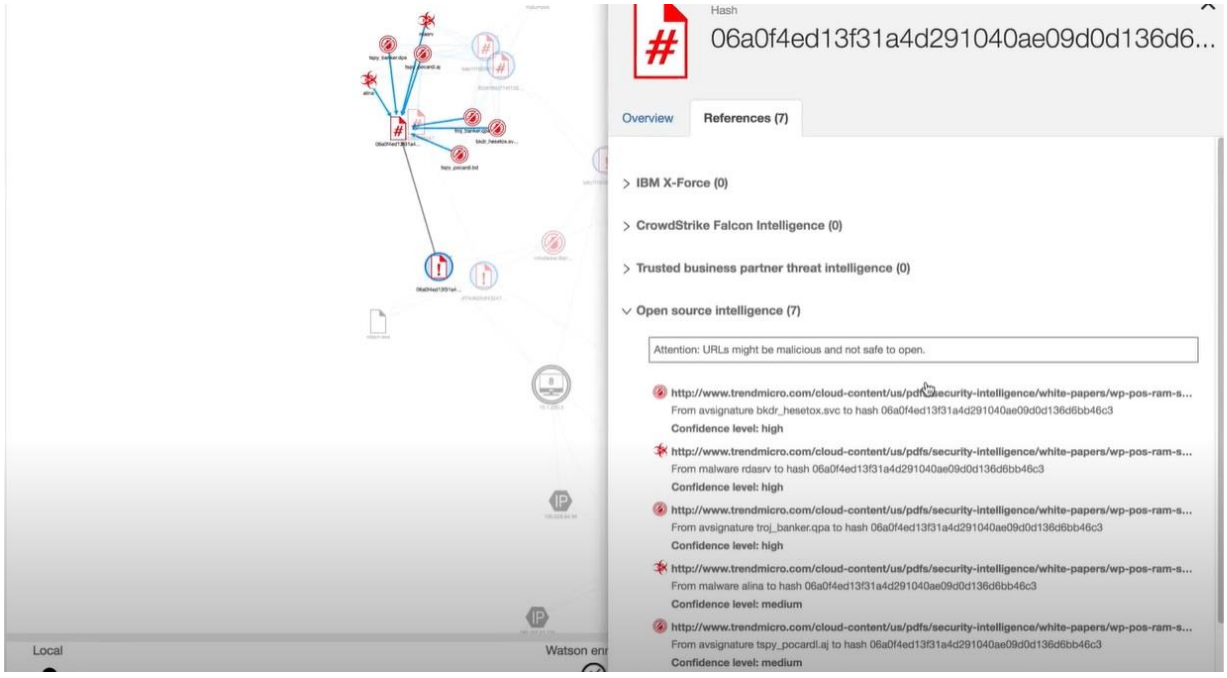

Рис. 3.8. Детальна інформація по загрозі

Таким чином враховуючи широкий спектр застосування Watson в корпоративних інформаційних системах різних галузях та напрямках, можна зробити висновок, про доцільність застосування такої системи, яка призводить до поліпшення інформаційного захисту, за рахунок проведення детального розслідування причин та їх наслідків спричинених кіберінцидентами.

Надає рекомендації відносно таких кіберінцидентів.

3.3 Рекомендації щодо застосування технології штучного інтелекту в кібер безпеці

Класифікація продуктів з технологіями штучного інтелекту за сценаріями застосування

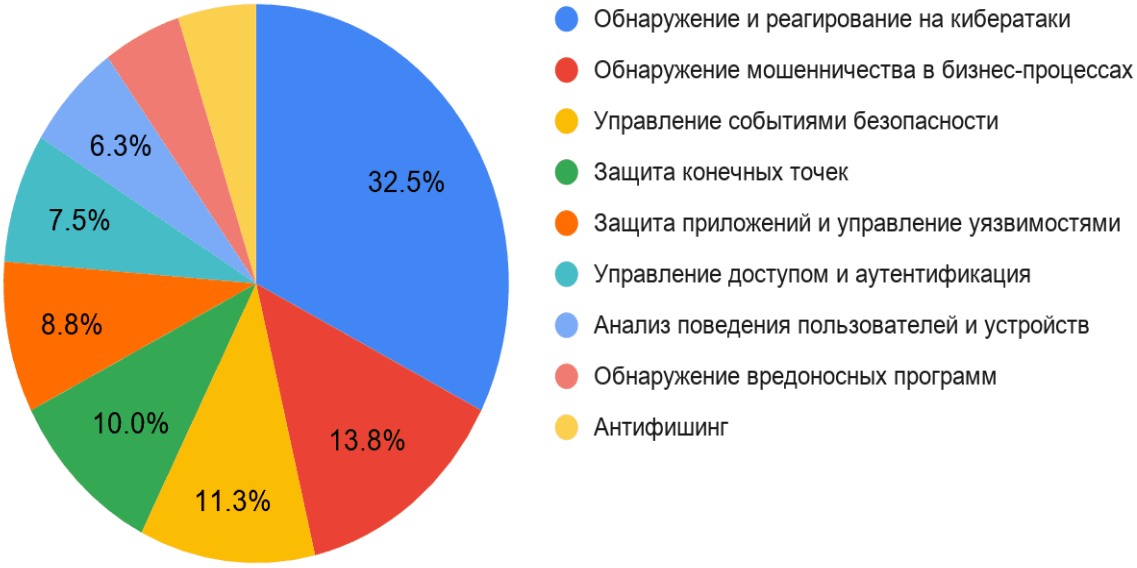

Рис 3.9. Розподіл продуктів із застосуванням технологій ШІ за сценаріями використання

Перелічимо основні типи:

1. EDR (Endpoint Detection and Response) - платформи виявлення атак на робочих станціях, серверах, будь-яких комп'ютерних пристроях (кінцевих точках) і оперативного реагування на них. За допомогою технологій ІІ продукти даної

категорії можуть виявляти невідомі шкідливі програми, автоматично класифікувати загрози і самостійно реагувати на них, передаючи дані в центр управління. ІІ приймає рішення на основі загальної бази знань, накопиченої шляхом збору даних зі безлічі пристроїв. Деякі продукти даного типу використовують технології ІІ для розмітки даних на кінцевих точках і подальшого контролю їх переміщення, щоб виявляти внутрішні загрози.

2. NDR (Network Detection and Response) - пристрої і аналітичні платформи, які виявляють атаки на мережевому рівні і дозволяють оперативно на них реагувати. Використовуючи накопичену статистику і базу знань про загрози, продукти даного типу виявляють за допомогою технологій ІІ загрози в мережевому трафіку і можуть автоматично на них реагувати належним чином, змінюючи конфігурацію мережевих пристроїв і шлюзів. Частина продуктів даного типу спеціалізується на захисті хмарних провайдерів і їх інфраструктури. Додатковий сценарій використання ІІ в мережевий захист - це аналіз поштового трафіку на предмет фішингу.

3. UEBA (User and Entity Behavior Analytics) - системи поведінкового аналізу користувачів і інформаційних сутностей. Вони виявляють випадки незвичайного поведінки і використовують їх для детектування внутрішніх і зовнішніх загроз. Основний сценарій застосування ІІ-технологій в продуктах типу UEBA - це автоматичне виявлення аномалій в поведінкових моделях (відхилення від норми або відповідність шаблону (патерни) загрози) для користувачів і різних сутностей інформаційних систем. Виявлені аномалії класифікуються за допомогою ІІ як різні загрози і ризики для бізнесу. Аномальна поведінка може виявлятися в цілях моніторингу та управління доступом, виявлення шахрайства серед клієнтів або співробітників (антіфрод), захисту конфіденційних даних, перевірки дотримання тих чи інших регламентів і нормативних актів.

4. TIP (Threat Intelligence Platform) -платформи раннього детектування загроз і реагування на них, що діють на основі великої кількості різних даних (Data Lake) і індикаторів компрометації (IoC) .Прімененіе II дозволяє підвищити ефективність виявлення невідомих загроз на ранніх етапах; сценарій дуже схожий з роботою SIEM-систем, але націлений на зовнішні джерела даних і зовнішні загрози.

5. SIEM (Security Information and Event Management) - рішення, які здійснюють моніторинг інформаційних систем, в режимі реального часу аналізують події безпеки, що надходять від мережевих пристроїв, засобів захисту інформації, IT-сервісів, інфраструктури систем і додатків, і допомагають виявити інциденти ІБ. У системах такого класу накопичується величезна кількість даних з різних джерел, а застосування технологій II дає можливість виявлення аномалій евристичними методами і скорочення помилкових спрацьовувань при зміні патернів і моделей даних. Застосування II в SIEM-системах дозволяє досягти дуже високого рівня автоматизації.

6. SOAR (Security Orchestration and Automated Response) - системи, що дозволяють виявляти загрози інформаційній безпеці і автоматизувати реагування на інциденти. У рішеннях даного типу, на відміну від SIEM-систем, II допомагає не тільки проводити аналіз, а й автоматично реагувати належним чином на виявлення загрози.

7. Засоби захисту додатків (Application Security) - системи, що дозволяють визначати загрози безпеки прикладних програм, керувати подальшим циклом моніторингу та усунення таких загроз. Основний сценарій застосування технологій II в системах захисту прикладних програм - автоматичний збір інформації про уразливість, атаках і заражених, доступною в відкритих джерелах, і заснована на його результатах автоматизація захисних дій: сканування на уразливості, зміни правил захисту для веб-додатків, виявлення

загроз і зміни ризикової моделі.

8. Антіфрод (Antifraud) - системи, що дозволяють виявляти загрози в бізнес-процесах і запобігати шахрайські операції в режимі реального часу. У системах захисту від шахрайства технології II застосовуються для визначення відхилень від встановлених бізнес-процесів, тим самим допомагаючи швидко реагувати на можливе фінансове злочин або вразливість процесів. Застосування II в таких системах особливо актуально, так як дозволяє швидко адаптуватися до зміни логіки і різних метрик бізнес-процесів, а також використовувати кращі практики в індустрії.

Для всіх типів даних систем технології штучного інтелекту дозволяють збільшити ефективність детектування невідомих загроз. Так вважають, за даними SANS, близько 30% фахівців з безпеки.

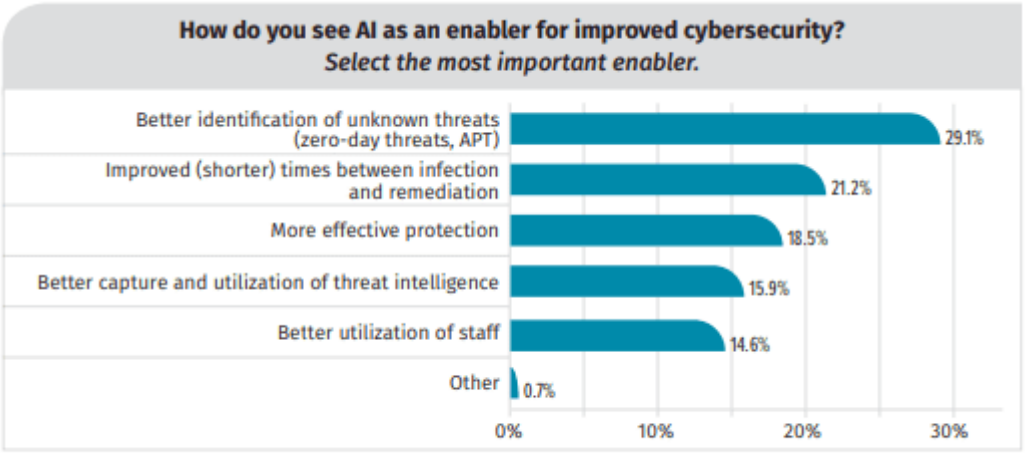

Рис. 3.10 Які метрики інформаційної безпеки поліпшить застосування технологій ШІ

Benefits	All Orgs	Orgs w/max of 10% AI	Orgs w/>10% AI
AI makes investigation of alerts faster	**60%**	49%	69%
AI improves the efficiency of our security staff	**60%**	46%	70%
Automatic initial triage	**49%**	41%	54%
Optimize threat identification	**47%**	41%	51%
AI speeds the remediation of threats	**44%**	33%	53%
AI helps to reduce false positives	**38%**	28%	47%
Automatic remediation or isolation	**23%**	17%	28%

Source: Osterman Research, Inc.

Рис. 3.11. Статистика щодо поліпшення показників інформаційної безпеки після застосування технологій ШІ

Висновки

Штучний інтелект вносить помітний внесок в боротьбу з сучасними інформаційними загрозами. Зокрема, в більшості випадків впровадження технологій ІІ в інформаційній безпеці організації скорочує час виявлення проблем та реагування на інциденти, а також витрати на управління персоналом. Експлуатанти відзначають зростання ефективності детектування невідомих загроз, а також швидкості аналізу і виявлення шкідливої активності на кінцевих точках і в додатках.

Сумарні інвестиції в компанії, які створюють продукти з інформаційної безпеки з застосуванням технологій ШІ, складають $ 3749 мільйонів на кінець 2019 року. При цьому світовий ринок продуктів з інформаційної безпеки з застосуванням технологій ШІ досягне $ 30 млрд в 2025 році з щорічним зростанням на 23%.[14]

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми розслідування кібер інцидентів корпоративної інформаційної системи, встановлена сутність завдань їх захисту.

Проаналізовано існуючі технології розслідування кібер інцидентів корпоративної інформаційної системи. Досліджена технологія розслідування кібер інцидентів корпоративної інформаційної системи на базі платформи Qradar Adwisor Watson.

Визначено методи та засоби розслідування кібер інцидентів, які реалізовані в Qradar Adwisor Watson.

Встановлено основні функції та принципи роботи платформи Qradar Adwisor Watson. Платформа Watson for Cyber Security оперує в своїй роботи даними з 100 000 задокументованих вразливостей ПЗ, що містяться в базі даних IBM X-Force Exchange. Також в розпорядженні когнітивної системи більше 10 000 різних документів і 700 000 записів в блогах фахівців з інформаційної безпеки, що публікуються щороку. У разі необхідності всі ці дані можна швидко структурувати і отримати необхідну інформацію з певної тематики. Структуровані дані, сформовані Watson for CyberSecurity, надходять в сервіс IBM QRadar,

ПЕРЕЛІК ПОСИЛАНЬ

1. Брюске, Д.Я., Савельев, А.Ю. Архитектура корпоративных информационных систем (web-формат) [Электронный ресурс. Мультимедиа]. Учебное пособие. Тамбов. Издательство ФГБОУ ВО "ТГТУ", 2018.

2. Моделі і методи проектування інформаційних систем. Проектування інформаційних систем. Архітектура інформаційних систем [Електронний ресурс] – Режим доступу: https://elearning.sumdu.edu.ua/free_content/lectured:de1c9452f2a161439391120eef364dd8ce4d8e5e/20151220200610/170352/index.html#p1.

3. Томашевський О.М. Інформаційні технології та моделювання бізнес-процесів: навч. посіб. / О.М. Томашевський, Г.Г. Цегелик, М.Б. Вітер, В.І. Дубук // – К. : ЦУЛ, 2012. – 296 с.

4. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004. – 384 с.

1. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ-Петербург – Арлит, 2002. – 496 с.

2. Леонтьев В.П. Безопасность в сети Интернет. – М.: ОЛМА Медиа Групп, 2008. – 256 с.

3. Гульев И.А. Компьютерные вирусы, взгляд изнутри. – М.: ДМК, 1998. – 304 с

4. [Електроний ресурс] Режим доступу https://studfiles.net/preview/5118185/page:42/

5. [Електронний ресурс] IBM Watson и кибербезопасность: служба быстрого реагирования, которая работает круглосуточно / Блог компании IBM / Хабр (habr.com)

6. [Електронний ресурс] : https://www.anti-malware.ru/news/2017-02-14/22220

7. [Електронний ресурс] www.csis.org/programs/strategic-technologies-program/significant-

8. [Електронний ресурс] Investigate Threats with Watson: QRadar Use Case demo video (seismic.com)

9. [Електронний ресурс] Security Gets Smart with AI (sans.org)

10. [Електронний ресурс] https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security#part4

11. [Електронний ресурс] Искусственный интеллект в кибербезопасности | DOU